S. HRG. 109–61

CURRENT AND PROJECTED NATIONAL SECURITY THREATS TO THE UNITED STATES

HEARING

BEFORE THE

SELECT COMMITTEE ON INTELLIGENCE UNITED STATES SENATE

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

FEBRUARY 16, 2005

Printed for the use of the Select Committee on Intelligence

Available via the World Wide Web: http://www.access.gpo.gov/congress/senate

U.S. GOVERNMENT PRINTING OFFICE

22–379 PDF WASHINGTON : 2005

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) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

SELECT COMMITTEE ON INTELLIGENCE

[Established by S. Res. 400, 94th Cong., 2d Sess.]

PAT ROBERTS, Kansas, *Chairman*
JOHN D. ROCKEFELLER IV, West Virginia, *Vice Chairman*

ORRIN G. HATCH, Utah
MIKE DeWINE, Ohio
CHRISTOPHER S. BOND, Missouri
TRENT LOTT, Mississippi
OLYMPIA J. SNOWE, Maine
CHUCK HAGEL, Nebraska
SAXBY CHAMBLISS, Georgia

CARL LEVIN, Michigan
DIANNE FEINSTEIN, California
RON WYDEN, Oregon
EVAN BAYH, Indiana
BARBARA A. MIKULSKI, Maryland
JON S. CORZINE, New Jersey

BILL FRIST, Tennessee, *Ex Officio*
HARRY REID, Nevada, *Ex Officio*
JOHN WARNER, Virginia, *Ex Officio*

BILL DUHNKE, *Staff Director and Chief Counsel*
ANDREW W. JOHNSON, *Minority Staff Director*
KATHLEEN P. MCGHEE, *Chief Clerk*

CONTENTS

CURRENT AND PROJECTED NATIONAL SECURITY THREATS TO THE UNITED STATES

WEDNESDAY, FEBRUARY 16, 2005

UNITED STATES SENATE,
SENATE SELECT COMMITTEE ON INTELLIGENCE,
Washington, DC.

The Committee met, pursuant to notice, at 10:03 a.m., in room SH–216, Hart Senate Office Building, the Honorable Pat Roberts, Chairman of the Committee, presiding.

Committee Members Present: Senators Roberts, Hatch, Bond, Lot, Snowe, Chambliss, Warner, Rockefeller, Levin, Feinstein, Wyden, Bayh, and Mikulski.

OPENING STATEMENT OF THE HONORABLE PAT ROBERTS, CHAIRMAN

Chairman ROBERTS. The hearing will come to order.

Today, the Senate Committee on Intelligence meets in open session to conduct its annual worldwide threat hearing. I would like to inform Members that traditionally we have a closed hearing in the afternoon, but Secretary of State Rice is coming to the Senate to brief all Members this afternoon.

We will follow up with individuals at our weekly intelligence hearings, and then, obviously, a hearing or briefing at any Member's request. So we will see all of these people back again in a classified session at another time.

The Committee traditionally begins its annual oversight of the U.S. intelligence community with an open hearing, so that the public will have the benefit of the intelligence community's best assessment of the current and projected national security threats to the United States.

Our witnesses today are Mr. Porter Goss, the Director of Central Intelligence. Welcome back, Mr. Director.

Director GOSS. Thank you, Mr. Chairman.

Chairman ROBERTS. Mr. Robert Mueller, the Director of the Federal Bureau of Investigation; Admiral James Loy, the Deputy Secretary of the Department of Homeland Security; Vice Admiral Lowell Jacoby, the Director of the Defense Intelligence Agency; and Ms. Carol Rodley, the Principal Deputy Assistant Secretary of State for Intelligence and Research. The acronym for that, by the way, is INR.

The Committee thanks all of our distinguished witnesses for being here today. We thank you for your commitment, for your perseverance on your job, and for helping to keep America safe.

Before we begin the testimony, I would like to take this opportunity to discuss an issue that has concerned and frustrated me since I joined this Committee over 8 year ago, and all Members of this Committee from time to time.

While we meet today in open session, the Members of this Committee and our witnesses will be limited in what they can say because the vast majority of the information with which this Committee and our witnesses deal is classified. The issues which we cover are not necessarily secret, but the details that surround them generally are.

Our goal today is to have as open a discussion as possible, recognizing that there are simply some things that we cannot and must not discuss publicly. The dynamics surrounding what we can and cannot say represents one of the most frustrating aspects of membership on this Committee, especially when secret intelligence activities find their way into public discourse.

How do we as a Committee assure the American people that we are even aware of something when we cannot discuss it publicly? How, without confirming or denying a particular story, do we explain that concerns are misplaced, on point or off point? Where do we draw the line between the public's right to know and our Nation's security interests in keeping something secret? These remain very difficult questions.

In 1976, the U.S. Senate established this Committee to conduct vigorous oversight of the intelligence activities of the United States government. And that is exactly what we do, day in and day out—with, I might add—what the Vice Chairman and I consider to be an outstanding and most capable staff.

Unfortunately, but necessarily, the Members of this Committee are rarely at liberty to respond to public stories or to inquiries. This does not mean, however, that we are not aware of or deeply involved in the issue that is being discussed.

Much of this Committee's work gets done behind closed doors with little fanfare. And open public discussion about all of the issues on which our Committee works is just not possible. If we were to discuss some of the ingenious ways this Nation does collect intelligence and protects our citizens, our adversaries would and could develop simple countermeasures that would eliminate these advantages, which were developed at great cost or high risk. This secrecy does protect lives and helps us to keep safe.

The Vice Chairman and I will, however, continue to work together to keep the American people as informed as possible. And when we can, we will do our best to clarify any misconceptions that may exist. With that in mind, I will now briefly discuss some of our plans for this Committee's oversight in the coming months.

First, we look forward to the naming of a Director of National Intelligence. As soon as the President nominates this individual, we will schedule a confirmation hearing as soon as practicable.

Second, we will monitor closely the implementation of the Intelligence reform bill. We will focus a great deal of attention on how this Committee can support the new DNI in the exercise of his or her authorities. And, because no legislation is perfect, we will also look at whether any legislative fixes are necessary.

Third, in the area of oversight, we will focus on the intelligence community's collection and analytical capabilities, especially in regard to our capabilities. Do we have the adequate collection? Do we have the adequate analysis? Do we have the information access to make a consensus threat analysis that is both credible and helpful to the policymakers and the Congress?

This Committee learned from our Iraq WMD inquiry that we cannot and should not always take the intelligence community's assessments at face value. The Vice Chairman and I have therefore decided to change the way the Senate Intelligence Committee does our work.

We haven't launched anything. We haven't really begun an investigation or an inquiry. Nor have we ruled them out. We have simply adjusted our approach based on the lessons we learned while reviewing the assessment by the community on Iraq's WMD programs.

Applying the methodologies that we used in that review, we will now look deeper into the intelligence community's work on the very critical threats that face our Nation. Instead of examining these issues after the fact, as we did on the Iraq WMD question and many other matters in the past, we are going to be more proactive, to try to identify our strengths and our weaknesses ahead of time. We have already begun to examine our intelligence capabilities with respect to nuclear terrorism and also the country of Iran.

In closing, I want to say something about the limitations of intelligence. Even the best intelligence will not be absolutely precise and tell us what to do. However, intelligence is a necessary and crucial tool used by policymakers to make very difficult decisions that do directly affect those who defend our freedoms and our national security.

With that said, I look forward to the testimony of our witnesses, and also the questions by our Members. I now turn to the distinguished Vice Chairman for any comment he may wish to make.

Senator Rockefeller.

STATEMENT OF THE HONORABLE JOHN D. ROCKEFELLER IV, VICE CHAIRMAN

Vice Chairman ROCKEFELLER. Thank you, Mr. Chairman.

It's customary at the beginning of our hearings to welcome everybody, and I certainly do so, and very much look forward to your testimony. I have to say, though, I think there is a significant absence or an empty spot at the table, at the witness table. And I want to talk about that.

There should be another chair before us. And the little sign in front of it should read Director of National Intelligence, DNI. Last summer, the Congress made reforming the intelligence community its top legislative priority. We worked through our August recess. We came back in a lame duck session after the election.

And we eventually passed landmark legislation fundamentally reforming the intelligence community for the first time in 50 years. The Congress made this extraordinary effort because it believed that our Nation was at risk, and we take that seriously.

More specifically, the Congress—eventually joined by the President—understood that without one individual in charge of the 15-agency intelligence community, America's war on terrorism would continue to be hampered by bureaucratic infighting and by budgetary tug-of-wars, that in turn inhibit the sharing of information—or, as we like to say, the access to information—and limit our ability to bring all of our resources to bear on what is a fairly ghastly threat on a worldwide basis.

When the President signed the intelligence reform bill in December, I really expected that when this hearing came the new Director of National Intelligence would be here to talk about threats.

It took 3 months for the Senate and the House to pass separate intelligence bills—that's not really very much time—and then resolve a multitude of differences in conference and all kinds of back-and-forth in a way which was agreeable to the Administration.

Two months have now passed since the bill-signing ceremony. And the position of Director of National Intelligence remains vacant—not even a person nominated. To me, this is unacceptable. It's unacceptable that the Administration has not shown the same urgency in dealing with that question that the Congress took the trouble to create. Some agree, some don't agree with the decision, but it was not a particularly close vote in either house.

With absolutely no disrespect—and, in fact, a great deal of respect to Director Goss—or any of our other witnesses, it is unacceptable that we cannot hear from and question the one person under the new law that is supposed to be responsible for the overall management of how the intelligence community is responding to the national security threats that we will be discussing this morning.

There are other troubling consequences to the Administration's lack of action. In recent weeks, I visited most of the principal agencies that comprise our intelligence community. The message I heard over and over, through words or body language, was that the senior leadership at these agencies was—that action on how best to carry out some key provisions on the intelligence reform bill was being held up pending the arrival of the new Director of National Intelligence. The delay in appointing a DNI has kept implementation of the reform bill, therefore, in my judgment, in idle.

So, what are the practical consequences of this delay, in the context of today's threat hearing? I'll highlight three.

The first and most obvious is that delaying the appointment of the DNI places that individual at a growing disadvantage in establishing his or her team—the new directorate—and selecting his or her supporting team of deputies within the 6 months prescribed by law, 2 months already having gone by, or more. It's prescribed by law, has to have it done.

The second consequence of delay pertains to the intelligence community's counterterrorism program. In addition to establishing the position of DNI, the intelligence reform bill mandated the creation of the National Counterterrorism Center, or NCTC. Initially created by Executive Order, the NCTC is chartered to be the primary organization in the U.S. Government responsible for analyzing and integrating all intelligence pertaining to terrorism and counterterrorism.

As is the case with the DNI, the head of the NCTC is a Senate-confirmed position and the Administration has yet to nominate a person to carry out those crucial tasks. One could say one has to do the DNI before the NCTC, but let's get going.

One of the primary missions of the NCTC—and I'm reading the law now—is to conduct strategic operational planning for counterterrorism activities, integrating all instruments of national power, including diplomatic, financial, military, intelligence activities, as well as homeland security and law enforcement activities, and to assign roles and responsibilities as part of its strategic operational planning.

My understanding is that the operational planning mission at NCTC is not being undertaken, pending confirmation of the new DNI. We can discuss that. So when we talk about going after terrorists, after their organizations, where they plot and where they train and where they keep their money, the question is, who is carrying out this strategic operational planning mission on this day?

In the wake of our war against the al-Qa'ida terrorist network and its operational bases in Afghanistan and Pakistan, the fundamentalist Islamic terrorist threat has splintered and decentralized its operations. We need a person in charge, we need an organization in place, that can coordinate counterterrorist operations across agencies against this multiplying terrorist threat.

The third immediate consequence of not having a DNI in place is the area of proliferation of weapons of mass destruction. The proliferation activity of North Korea and Iran, along with the damage done by Pakistani scientist A.Q. Khan, has reduced any confidence that the nuclear genie is contained.

The combination of these two threats—a decentralized, but determined terrorist threat and growing proliferation activity—present the intelligence community with a sobering challenge, now and for the foreseeable future.

The Congress recognized the importance of this challenge in crafting the intelligence reform bill, by authorizing the establishment of a National Counterproliferation Center. The new intelligence center would generally follow the blueprint of the National Counterterrorism Center. Again, I am told and troubled by the fact that the decision on whether or not to establish the National Counterproliferation Center and, if so, in what form, is being held up pending the DNI's appointment.

The proliferation activities of North Korea are a threat to our security and the security of our allies today, as well as down the road. And the same, of course, is true with Iran, and we discover others as we go along. Iran, as a nuclear aspirant and supporter of terrorism, is also center stage and very much needs to be pursued in this manner.

Policymakers and, most importantly, the President, but also the Congress, need the best intelligence possible on North Korea, Iran and other hotspots around the world—Africa being one which I may ask a question about.

The faulty intelligence used by the Administration to invade Iraq has harmed our credibility with our allies and has given Islamic jihadists a powerful recruiting tool around the world that is not to anybody's advantage. We must learn from these mistakes, as the

Chairman has indicated, and get better in how we produce timely, objective and accurate intelligence for U.S. policymakers.

The Chairman and I have directed that the Intelligence Committee undertake review of how intelligence on Iran is collected, analyzed and produced. The review will be similar to what we did before with weapons of mass destruction in Iraq. But it's going to be very proactive. The same sort of rigorous oversight ought to apply to North Korea also, and there are some other countries that come to mind.

I am hopeful that the Committee can also focus the efforts of its very talented staff on the growing controversy surrounding the collection of intelligence through the interrogation and rendition of detainees. We need to probe the fundamental legal, jurisdictional and operational questions, both retrospectively and prospectively, in my mind, at the heart of how the intelligence community collects such intelligence.

It's undeniable that the intelligence community has made enormous strides in the past 3 years and that some reform has occurred. The tireless efforts of hardworking men and women at the CIA, FBI and other intelligence agencies, like the work of those in uniform, have been a linchpin in the effort to protect every American against the murderous intentions of terrorists.

But there is an acknowledgement among the people I have spoken with that we can do better and that we must get better. The intelligence reform bill addressed that issue of authorities, resources and organization. But the promise of reform will not be realized without strong leadership and management acumen—the sort of skills the DNI must bring to the table.

Challenges abound, as the Chairman knows, for the current and future leadership of the intelligence community. There's a lot of work to be done on how we collect intelligence, particularly in the arena of human intelligence, analytical workforce problems, language problems. Our intelligence community needs to establish a global presence that is not only capable, but lithe, for our adversaries are increasingly mobile and use much more sophisticated technology as they do their work.

I know we're limited as to what we can discuss in an open hearing, but I hope to the extent possible that our witnesses will address some of the questions that I have raised.

I thank the witnesses and I thank you, Mr. Chairman.

Chairman ROBERTS. Before I recognize Director Goss, I would like to speak to the Vice Chairman's comments in regard to the appointment of a DNI. I think this is what we used to hear on "Perry Mason," with extenuating circumstances.

The intelligence reform bill was passed on December 17. The bill says that a DNI will be appointed no later than 6 months—that is, June 17. I think, or at least it is my opinion, that the Administration is also awaiting the report of the independent WMD commission, part of whose job or task is to take a look at the intelligence reform bill and make some recommendations.

In addition, while I share the Vice Chairman's frustration that we wish we had here the Director of National Intelligence and that he or she was well down the road to implementing the reform bill, it is, I think, crucially important, not only in terms of timing, but

to get the right person. And that person should have managerial experience, obviously, expertise in intelligence, obviously, expertise and experience perhaps in the military. As the Vice Chairman has pointed out, we have certainly people in the Washington area or, for that matter, within the United States, that certainly fit that description.

So, I hope that the Administration will move in an expeditious fashion, but in a fashion that gets the right person for the job.

Director Goss, you may proceed, sir.

STATEMENT OF THE HONORABLE PORTER J. GOSS, DIRECTOR OF CENTRAL INTELLIGENCE

Director GOSS. Thank you very much, Mr. Chairman. Good morning, Mr. Vice Chairman and Members of the Committee, and thank you for the hospitable welcome here.

The challenges that you've mentioned in your opening remarks that face the United States of America and its citizens and our interests literally do span the globe. My intention today is to tell you what I believe are those challenges in terms of the most threatening and identify briefly where we think our service as intelligence professionals is needed most on behalf of the United States taxpayers.

We need to make some tough decisions about which haystacks deserve to be scrutinized for the needles that can hurt us most. And we know in this information age that there are literally endless haystacks everywhere. There's an awful lot of material out there.

I do want to make several things clear. Our officers are taking risks, and I will be asking them to take more risks—justifiable risks—because I would be much happier here explaining why we did something than why we did nothing.

I'm asking for more competitive analysis, more co-location of analysts and collectors—in fact, that's underway—and deeper collaboration with agencies throughout the intelligence community.

Above all, our analysts must be objective. Our credibility rests there, as you pointed out well in this Committee's report to the community issued on the WMD.

We do not make policy. We do not wage war. I am emphatic about that. I testified to that during my confirmation, and it is still true and it will always be. We do collect and analyze information. With respect to the CIA, I want to tell you that my first few months as Director have served only to confirm what I and, I think, Members of Congress have known about CIA for years. It is a special place. It's an organization of dedicated, patriotic people who are doing their best.

In addition to taking a thorough, hard look at our own capabilities, we're working to define CIA's place in the restructured intelligence community—a community that will be led by a new DNI, as we've heard—to make the maximum possible contribution to American security at home and abroad that uniquely the CIA can make.

The CIA is and will remain the flagship agency, in my view, and each of the other 14 elements of the community will continue to

make their unique contributions, as well. I say that as the DCI, not as the Director of Central Intelligence Agency.

I turn to threats. I will not attempt, obviously, to cover everything that could go wrong in the year ahead. We must and do concentrate our efforts, experience and expertise on the challenges that are most pressing. And they are, of course, defeating terrorism, protecting the homeland, stopping proliferation of weapons of mass destruction and drugs, fostering stability, freedom and peace in the most troubled regions of the world.

My comments today will focus on these duties. I know well from my 30 years in public service that you and your colleagues have an important responsibility with these open sessions to get information to the American people, as the Chairman has stated.

I also know too well, as the Chairman has stated, that as we are broadcasting to America, enemies are also tuning in. In open session, I feel that I will and must be very prudent in my remarks as DCI.

Mr. Chairman, on the subject of terrorism, defeating terrorism must remain one of our intelligence community's core objectives, and it will, as widely dispersed terrorist networks will present one of the most serious challenges to the U.S. national security interests at home and abroad in the coming year. That's not startling news, but it's important.

In the past year, aggressive measures by our intelligence, law enforcement, defense and homeland security communities, along with our key international partners, have, in fact, dealt serious blows to al-Qa'ida and other terrorist organizations and individuals.

Despite these successes, however, the terrorist threat to the U.S. in the homeland and abroad endures. I'd make four points.

Al-Qa'ida is intent on finding ways to circumvent U.S. security enhancements to strike Americans in the homeland, one.

Number two, it may be only a matter of time before al-Qa'ida or another group attempts to use chemical, biological, radiological or nuclear weapons. We must focus on that.

Three, al-Qa'ida is only one facet of the threat from a broader Sunni jihadist movement.

And four, the Iraq conflict, while not a cause of extremism, has become a cause for extremists.

We know from experience that al-Qa'ida is a patient, persistent, imaginative, adaptive and dangerous opponent. But it is vulnerable and displaced. We and other allies have hit it hard. Jihadist religious leaders preach millennial, aberrational visions of some kind of a fight for Islam's survival. Sometimes they argue that the struggle justifies the indiscriminate killing of civilians, even with chemical, biological, radiological and nuclear weapons. And, fortunately, they have a small audience.

Our pursuit of al-Qa'ida and its most senior leaders, including bin Laden and his deputy, Ayman al-Zawahiri, is intense. However, their capture alone would not be enough to eliminate the terrorist threat to the U.S. homeland or interests overseas. Often influenced by al-Qa'ida's ideology, members of a broader movement have an ability to plan and conduct operations. We saw this last March in the railway attacks in Madrid, conducted by local Sunni extremists.

Other regional groups connected to al-Qa'ida or acting on their own also continue to pose a significant threat. In Pakistan, terrorist elements remain committed to attacking U.S. targets. In Saudi Arabia, remnants of the Saudi al-Qa'ida network continue to attack U.S. interests in the region.

In Central Asia, the Islamic Jihad Group, a splinter group of the Islamic Movement of Uzbekistan, has become a more virulent threat to U.S. interests and local governments there. Last spring, the group used female operatives in a series of bombings in Uzbekistan, as you know.

In Southeast Asia, the Jemaah Islamiyah continues to pose a threat to U.S. and Western interests in Indonesia and the Philippines, where JI is colluding with the Abu Sayyaf Group and possibly the MILF group, as well.

In Europe, Islamic extremists continue to plan and cause attacks against U.S. and local interests. Some of them may cause significant casualties. In 2004, British authorities dismantled an al-Qa'ida cell—much reported. And in the Netherlands, an extremist brutally killed a prominent Dutch citizen—not as widely reported.

Islamic extremists are exploiting the Iraqi conflict to recruit new, anti-U.S. jihadists. Those jihadists who survive will leave Iraq experienced and focused on acts of urban terrorism. They represent a potential pool of contacts to build transnational terrorist cells, groups and networks in Saudi Arabia, Jordan and other countries.

Zarqawi has sought to bring about the final victory of Islam over the West, in his version of it. And he hopes to establish a safe haven in Iraq from which his group could operate against the "infidel Western nations, the apostate Muslim governments."

Other groups spanning the globe also pose persistent and serious threats to U.S. and Western interests. Hizbollah's main focus remains Israel. But it could conduct lethal attacks against U.S. interests quickly upon a decision to do so. It has that capability, we estimate.

Palestinian terrorist organizations have apparently refrained from directly targeting U.S. or Western interests in their opposition to Middle East peace initiatives, but they do pose an ongoing risk to U.S. citizens that could be killed or wounded in attacks intended to strike Israeli interests.

Extremist groups in Latin America are still concerned with the FARC—the Revolutionary Armed Forces of Colombia—possessing capability and clear intent to threaten U.S. interests in that region.

The Horn of Africa, the Sahel, the Mahgreb, the Levant and the Gulf States are all areas where pop-up terrorist activity can be expected and needs to be monitored and dealt with.

Afghanistan, Mr. Chairman, once the safe haven for Usama bin Ladin, has started on the road to recovery after decades of instability and civil war. Hamid Karzai's election to the presidency was a major milestone. Elections for a new national assembly and local district councils, tentatively scheduled for this spring—though that's an ambitious schedule—will complete the process of electing representatives this year, hopefully. President Karzai still faces a low-level insurgency, aimed at destabilizing his country and raising the cost of reconstruction, and ultimately forcing coalition forces to leave before the job is done. The development of the Afghan na-

tional army and the national police force is going well, although neither can yet stand on its own.

In Iraq, low voter turnout in some Sunni areas and the post-election resumption of insurgent attacks—most against Iraqi civilian and security forces—indicate that the insurgency achieved at least some of its election day goals and remains a serious threat to creating a stable, representative government in Iraq.

Self-determination for the Iraqi people will largely depend on the ability of the Iraq forces to provide their own security. Iraq's most capable security units have become more effective in recent months, contributing to several major operations, and helping to put an Iraqi face on security operations. Insurgents are determined and still trying to discourage new recruits and undermine the effectiveness of existing Iraqi security forces by grotesque intimidation tactics.

The prolonged lack of security would hurt Iraq's reconstruction efforts and economic development, causing overall economic growth to proceed at a slower pace than many analysts expected and, certainly that the Iraqi people deserve.

Alternatively, the larger, uncommitted moderate Sunni population and the Sunni political elite may seize the post-electoral moment to take part in creating Iraq's new political institutions, if victorious Shia and Kurdish parties include Sunnis in the new government and the drafting of the constitution. That is a hopeful opportunity.

On the subject of proliferation, Mr. Chairman, I will now turn to the worldwide challenge. Last year started with promise, as Libya had just renounced its WMD programs, North Korea was engaged in negotiations with regional states on its nuclear weapons program, and Iran was showing greater signs of openness regarding its nuclear program after concealing activity for nearly a decade.

Let me start with Libya, which is a bit of a good news story and one that reflects the patient perseverance with which the intelligence community—writ large—can tackle a tough intelligence problem.

In 2004, Tripoli followed through with a range of steps to disarm itself of WMD and ballistic missiles. Libya gave up key elements of its nuclear weapons program and opened itself to the IAEA. Libya gave up some key CW assets, and opened its former CW program to international scrutiny.

After disclosing its Scud stockpile and extensive ballistic and cruise missile R&D efforts in 2003, Libya took the important step to abide by its commitment to limit its missiles to the 300-kilometer range threshold of the Missile Technology Control Regime.

Today, the U.S. continues to work with Libya to make sure that any discrepancies in the declarations they have made are clarified.

In North Korea, on the other hand, on 10 February 2005—not long ago—Pyongyang announced it was suspending participation in 6-party talks under way since 2003, declared it had nuclear weapons and affirmed it would seek to increase its nuclear arsenal. The North had been pushing for a freeze on its plutonium program in exchange for significant benefits rather than committing to the full dismantlement that we and our partners seek.

In 2003, the North claimed it had reprocessed the 8,000 fuel rods from the Yongbyon reactor, originally stored under the agreed framework, with the IAEA monitoring in 1994. The North claims to have made new weapons from its reprocessing effort.

We believe North Korea continues to pursue a uranium enrichment capability, drawing on the assistance it received from A.Q. Khan before his network was shut down.

North Korea continues to develop, produce, deploy and sell ballistic missiles of increasing range and sophistication, augmenting Pyongyang's large operational force of Scud and Nodong-class missiles. North Korea could resume flight testing at any time, including longer range missiles, such as the Taepo Dong–2 system. We assess the TD–2 is capable of reaching the United States with a nuclear weapon-size payload.

North Korea continues to market its ballistic missile technology, trying to find new clients now that some traditional customers—read Libya—have halted such trade.

We believe North Korea has active CW and BW programs, and probably has chemical and possibly biological weapons ready for use.

Iran. In early February, the spokesman of Iran's Supreme Council for National Security publicly announced that Iran would never scrap its nuclear program. This came in the midst of negotiations with EU–3 members—that would be Britain, Germany and France—seeking objective guarantees from Tehran that it would not use nuclear technology for nuclear weapons.

Previous comments by Iranian officials, including Iran's supreme leader and its foreign minister, indicated that Iran would not give up its ability to enrich uranium. Certainly, it would be right for Iran to have the capability to produce fuel for power reactors. But, we're more concerned about the dual-use nature of the technology that could also be used to achieve a nuclear weapon. We do not have transparency.

In parallel, Iran continues its pursuit of long-range ballistic missiles, such as an improved version of a 1,300-kilometer range Shahab–3 MRBM, to add to the hundreds of short-range Scud missiles it already has.

Even since 9/11, Tehran continues to support terrorist groups in the region, such as Hizbollah—it is a state sponsor—and could encourage increased attacks in Israel and the Palestinian territories to derail progress toward peace there. Iran reportedly is supporting some anti-coalition activities in Iraq and seeking to influence the future character of the Iraqi state.

Conservatives are likely to consolidate their power in Iran's June 2005 presidential elections, further marginalizing the reform movement of last year. Iran continues to retain, in secret, important members of al-Qa'ida, causing further uncertainty about Iran's commitment to bring them to justice one way or another.

Moving to China, Beijing's military modernization and military buildup could tilt the balance of power in the Taiwan Strait. Improved Chinese capabilities threaten U.S. forces in the region. In 2004, China increased its ballistic missile forces deployed across from Taiwan and rolled out several new submarines. China con-

tinues to develop more robust, survivable, nuclear-armed missiles, as well as conventional capability for use in regional conflict.

Taiwan continues to promote constitutional reform and other attempts to strengthen local identity. Beijing judges these moves to be a "timeline for independence." If Beijing decides that Taiwan is taking steps toward permanent separation that exceed Beijing's tolerance, we assess China is prepared to respond with varying levels of force.

China is increasingly confident and active on the international stage, trying to ensure it has a voice on major international issues, to secure access to natural resources, and to counter what it sees as United States efforts to contain or encircle it.

New leadership, under President Hu Jintao, is facing an array of domestic challenges in 2005, including the potential for a resurgence in inflation, increased dependence on exports, growing economic inequalities in the country, increased awareness of individual rights, and popular expectations for his new leadership.

In Russia, the attitudes and actions of the so-called "siloviki"—the ex-KGB men that Putin has placed in positions of authority throughout the Russian government—may be critical determinates of the course Putin will pursue in the year ahead. Perceived setbacks in Ukraine are likely to lead Putin to redouble his efforts to defend Russian interests abroad, while balancing cooperation with the West.

Russia's most immediate security threat is terrorism. And counterterrorism cooperation undoubtedly will continue.

Putin publicly acknowledges a role for outside powers to play in the confederate states, but we believe he is nevertheless concerned about further encroachment by the U.S. and NATO into that region.

Moscow worries that separatism inside Russia and radical Islamic movements beyond their borders might threaten stability in southern Russia. Chechen extremists have increasingly turned to terrorist operations in response to Moscow's successes in Chechnya, and it's reasonable to predict they will carry out attacks against civilian or military targets elsewhere in Russia in 2005.

Budget increases will help Russia create a professional military by replacing conscript with volunteer servicemen and focus on maintaining, modernizing and extending the operational life of strategic weapons systems, including the nuclear missile force.

Russia remains an important source of weapons technology, material and components for other nations. The vulnerability of Russian WMD materials and technology to theft or diversion is a continuing concern.

On other areas of potential instability, Mr. Chairman, I would briefly go to the Middle East.

The election of the Palestinian President, Mahmoud Abbas, marks an important step, and Abbas has made it clear that negotiating a peace deal with Israel is a very high priority. That's extraordinarily good news. Nevertheless, there are hurdles ahead.

Redlines must be resolved while the Palestinian leaders try to rebuild damaged PA infrastructure and governing institutions, especially the security forces, the legislature and the judiciary—those things that will help stability. Terrorist groups, some of whom ben-

efit from funding from outside sources, could step up attacks to derail peace and progress and need close monitoring.

In Africa, chronic instability will continue to hamper counterterrorism efforts and impose heavy humanitarian and peacekeeping burdens on us.

In Nigeria, the military is struggling to contain militia groups in the oil-producing south and ethnic violence that frequently erupts throughout the country. Extremist groups are emerging from the country's Muslim population of about 65 million. Nigeria is a big oil producer for us.

In Sudan, the peace deal signed in January will result in de facto southern autonomy and may inspire rebels in provinces such as Darfur to press harder for a greater share of resource and power. Opportunities exist for Islamic extremists to reassert themselves in the north, unless the central government stays unified.

Unresolved disputes in the Horn of Africa—Africa's gateway to the Middle East—create vulnerability to foreign terrorists and extremist groups. Ethiopia and Eritrea still have a contested border. And armed factions in Somalia indicate they will fight the authority of a new transitional government.

In Latin America, the region is entering a major electoral cycle in 2006. Brazil, Colombia, Costa Rica, Ecuador, Mexico, Nicaragua, Peru and Venezuela hold presidential elections.

Several key countries in the hemisphere are potential flashpoints in 2005. In Venezuela, Chavez is consolidating his power by using technically legal tactics to target his opponents and meddling in the region, supported by Castro.

In Colombia, progress against counternarcotics and terrorism under President Uribe's successful leadership may be affected by an election.

The outlook is very cloudy for legitimate, timely elections in November 2005 in Haiti, even with substantial international support.

Campaigning for the 2006 presidential election in Mexico is likely to stall progress on fiscal, labor and energy reform.

And in Cuba, Castro's hold on power remains firm. But a bad fall last October has rekindled speculation about his declining health and the succession scenarios.

In Southeast Asia, three countries bear close watching. In Indonesia, President Yudhoyono has moved swiftly to crack down on corruption. But reinvigorating the economy, burned by the cost of recovery in the tsunami-damaged area, will likely be affected by continuing, deep-seated ethnic and political turmoil exploitable by terrorists.

In the Philippines, Manila is struggling with prolonged Islamic and Communist rebellion. The presence of Jemaah Islamiyah, terrorists seeking safe haven and training bases in the south, adds volatility and capability to terrorist groups already in place.

And finally, Mr. Chairman, Thailand is plagued with an increasingly volatile Muslim separatist threat in the southeastern provinces and the risk of escalation remains very high.

I thank you very much for that opportunity to give a brief overview.

[The prepared statement of Director Goss follows:]

PREPARED STATEMENT OF HON. PORTER GOSS,
DIRECTOR OF CENTRAL INTELLIGENCE

Good morning, Mr. Chairman, Mr. Vice Chairman, Members of the Committee.

It is my honor to meet with you today to discuss the challenges I see facing America and its interests in the months ahead. These challenges literally span the globe. My intention is to tell you what I believe are the greatest challenges we face today and those where our service as intelligence professionals is needed most on behalf of the U.S. taxpayer.

We need to make tough decisions about which haystacks deserve to be scrutinized for the needles that can hurt us most. And we know in this information age that there are endless haystacks everywhere. I do want to make several things clear:

• Our officers are taking risks, and I will be asking them to take more risks—justifiable risks—because I would much rather explain why we did something than why we did nothing,

• I am asking for more competitive analysis, more collocation of analysts and collectors, and deeper collaboration with agencies throughout the Intelligence Community. Above all, our analysis must be objective. Our credibility rests there.

• We do not make policy. We do not wage war. I am emphatic about that and always have been. We do collect and analyze information.

With respect to the CIA, I want to tell you that my first few months as Director have served only to confirm what I and Members of Congress have known about CIA for years. It is a special place—an organization of dedicated, patriotic people. In addition to taking a thorough, hard look at our own capabilities, we are working to define CIA's place in the restructured Intelligence Community—a community that will be led by a new Director of National Intelligence—to make the maximum possible contribution to American security at home and abroad. The CIA is and will remain the flagship agency, in my view. And each of the other 14 elements in the community will continue to make their unique contributions as well.

Now, I turn to threats. I will not attempt to cover everything that could go wrong in the year ahead. We must, and do, concentrate our efforts, experience and expertise on the challenges that are most pressing: defeating terrorism; protecting the homeland; stopping proliferation of weapons of mass destruction and drugs; and fostering stability, freedom and peace in the most troubled regions of the world. Accordingly, my comments today will focus on these duties. I know well from my 30 years in public service that you and your colleagues have an important responsibility with these open sessions to get information to the American people. But I also know all too well that as we are broadcasting to America, enemies are also tuning in. In open session I feel I must be very prudent in my remarks as DCI.

TERRORISM

Mr. Chairman, defeating terrorism must remain one of our intelligence community's core objectives, as widely dispersed terrorist networks will present one of the most serious challenges to U.S. national security interests at home and abroad in the coming year. In the past year, aggressive measures by our intelligence, law enforcement, defense and homeland security communities, along with our key international partners have dealt serious blows to al-Qa'ida and others. Despite these successes, however, the terrorist threat to the U.S. in the Homeland and abroad endures.

• Al-Qa'ida is intent on finding ways to circumvent U.S. security enhancements to strike Americans and the Homeland.

• It may be only a matter of time before al-Qa'ida or another group attempts to use chemical, biological, radiological, and nuclear weapons (CBRN).

• Al-Qa'ida is only one facet of the threat from a broader Sunni jihadist movement.

• The Iraq conflict, while not a cause of extremism, has become a cause for extremists.

We know from experience that al-Qa'ida is a patient, persistent, imaginative, adaptive and dangerous opponent. But it is vulnerable and we and other allies have hit it hard.

• Jihadist religious leaders preach millennial aberrational visions of a fight for Islam's survival. Sometimes they argue that the struggle justifies the indiscriminate killing of civilians, even with chemical, biological, radiological, or nuclear weapons.

Our pursuit of Al-Qa'ida and its most senior leaders, including Bin Ladin and his deputy, Ayman al-Zawahiri is intense. However, their capture alone would not be enough to eliminate the terrorist threat to the U.S. Homeland or U.S. interests overseas. Often influenced by al-Qa'ida's ideology, members of a broader movement have an ability to plan and conduct operations. We saw this last March in the railway

attacks in Madrid conducted by local Sunni extremists. Other regional groups—connected to al-Qa'ida or acting on their own—also continue to pose a significant threat.

• In Pakistan, terrorist elements remain committed to attacking U.S. targets. In Saudi Arabia, remnants of the Saudi al-Qa'ida network continue to attack U.S. interests in the region.

• In Central Asia, the Islamic Jihad Group (IJG), a splinter group of the Islamic Movement of Uzbekistan, has become a more virulent threat to U.S. interests and local governments. Last spring the group used female operatives in a series of bombings in Uzbekistan.

• In Southeast Asia, the Jemaah Islamiyah (JI) continues to pose a threat to U.S. and Western interests in Indonesia and the Philippines, where JI is colluding with the Abu Sayyaf Group and possibly the Mff.F.

• In Europe, Islamic extremists continue to plan and cause attacks against U.S. and local interests, some that may cause significant casualties. In 2004 British authorities dismantled an al-Qa'ida cell and an extremist brutally killed a prominent Dutch citizen in the Netherlands.

Islamic extremists are exploiting the Iraqi conflict to recruit new anti-U.S. jihadists.

• These jihadists who survive will leave Iraq experienced in and focused on acts of urban terrorism. They represent a potential pool of contacts to build transnational terrorist cells, groups, and networks in Saudi Arabia, Jordan and other countries.

• Zarqawi has sought to bring about the final victory of Islam over the West, and he hopes to establish a safe haven in Iraq from which his group could operate against "infidel" Western nations and "apostate" Muslim governments.

Other terrorist groups spanning the globe also pose persistent and serious threats to U.S. and Western interests.

• Hizballah's main focus remains Israel, but it could conduct lethal attacks against U.S. interests quickly upon a decision to do so.

• Palestinian terrorist organizations have apparently refrained from directly targeting U.S. or Western interests in their opposition to Middle East peace initiatives, but pose an ongoing risk to U.S. citizens that could be killed or wounded in attacks intended to strike Israeli interests.

• Extremist groups in Latin America are still a concern, with the FARC—the Revolutionary Armed Forces of Colombia—possessing the greatest capability and the clearest intent to threaten U.S. interests in the region.

• Horn of Africa, the Sahel, the Mahgreb, the Levant, and the Gulf States are all areas where "pop up" terrorist activity can be expected.

AFGHANISTAN

Mr. Chairman, Afghanistan, once the safe haven for Usama bin Ladin, has started on the road to recovery after decades of instability and civil war. Hamid Karzai's election to the presidency was a major milestone. Elections for a new National Assembly and local district councils—tentatively scheduled for this spring—will complete the process of electing representatives.

President Karzai still faces a low-level insurgency aimed at destabilizing the country, raising the cost of reconstruction and ultimately forcing Coalition forces to leave.

• The development of the Afghan National Army and a national police force is going well, although neither can yet stand on its own.

IRAQ

Low voter turnout in some Sunni areas and the post-election resumption of insurgent attacks—most against Iraqi civilian and security forces—indicate that the insurgency achieved at least some of its election-day goals and remains a serious threat to creating a stable representative government in Iraq.

Self-determination for the Iraqi people will largely depend on the ability of Iraqi forces to provide security. Iraq's most capable security units have become more effective in recent months, contributing to several major operations and helping to put an Iraqi face on security operations. Insurgents are determined to discourage new recruits and undermine the effectiveness of existing Iraqi security forces.

The lack of security is hurting Iraq's reconstruction efforts and economic development, causing overall economic growth to proceed at a much slower pace than many analysts expected a year ago.

• Alternatively, the larger uncommitted moderate Sunni population and the Sunni political elite may seize the post electoral moment to take part in creating

Iraq's new political institutions if victorious Shia and Kurdish parties include Sunnis in the new government and the drafting of the constitution.

PROLIFERATION

Mr. Chairman, I will now turn to the worldwide challenge of proliferation. Last year started with promise as Libya had just renounced its WMD programs, North Korea was engaged in negotiations with regional states on its nuclear weapons program, and Iran was showing greater signs of openness regarding its nuclear program after concealing activity for nearly a decade. Let me start with Libya, a good news story, and one that reflects the patient perseverance with which the Intelligence Community can tackle a tough intelligence problem.

LIBYA

In 2004, Tripoli followed through with a range of steps to disarm itself of WMD and ballistic missiles.

- Libya gave up key elements of its nuclear weapons program, opened itself to the IAEA.
- Libya gave up some key CW assets and opened its former CW program to international scrutiny.
- After disclosing its SCUD stockpile and extensive ballistic and cruise missile R&D efforts in 2003, Libya took important steps to abide by its commitment to limit its missiles to the 300-km range threshold of the Missile Technology Control Regime (MTCR).

The U.S. continues to work with Libya to clarify some discrepancies in the declaration.

NORTH KOREA

On 10 February 2005, Pyongyang announced it was suspending participation in the six-party talks underway since 2003, declared it had nuclear weapons, and affirmed it would seek to increase its nuclear arsenal. The North had been pushing for a freeze on its plutonium program in exchange for significant benefits, rather than committing to the full dismantlement that we and are our partners sought.

- In 2003, the North claimed it had reprocessed the 8,000 fuel rods from the Yongbyong reactor, originally stored under the Agreed Framework, with IAEA monitoring in 1994. The North claims to have made new weapons from its reprocessing effort.
- We believe North Korea continues to pursue a uranium enrichment capability drawing on the assistance it received from A.Q. Khan before his network was shutdown.

North Korea continues to develop, produce, deploy, and sell ballistic missiles of increasing range and sophistication, augmenting Pyongyang's large operational force of Scud and No Dong class missiles. North Korea could resume flight-testing at any time, including of longer-range missiles, such as the Taepo Dong-2 system. We assess the TD 2 is capable of reaching the United States with a nuclear-weapon-sized payload.

- North Korea continues to market its ballistic missile technology, trying to find new clients now that some traditional customers, such as Libya, have halted such trade.

We believe North Korea has active CW and BW programs and probably has chemical and possibly biological weapons ready for use.

IRAN

In early February, the spokesman of Iran's Supreme Council for National Security publicly announced that Iran would never scrap its nuclear program. This came in the midst of negotiations with EU-3 members (Britain, Germany and France) seeking objective guarantees from Tehran that it will not use nuclear technology for nuclear weapons.

- Previous comments by Iranian officials, including Iran's Supreme Leader and its Foreign Minister, indicated that Iran would not give up its ability to enrich uranium. Certainly they can use it to produce fuel for power reactors. We are more concerned about the dual-use nature of the technology that could also be used to achieve a nuclear weapon.

In parallel, Iran continues its pursuit of long-range ballistic missiles, such as an improved version of its 1,300 km range Shahab-3 MRBM, to add to the hundreds of short-range SCUD missiles it already has.

Even since 9/11, Tehran continues to support terrorist groups in the region, such as Hizballah, and could encourage increased attacks in Israel and the Palestinian Territories to derail progress toward peace.

• Iran reportedly is supporting some anti-Coalition activities in Iraq and seeking to influence the future character of the Iraqi state.

• Conservatives are likely to consolidate their power in Iran's June 2005 presidential elections, further marginalizing the reform movement last year.

• Iran continues to retain in secret important members of Al-Qai'ida—the Management Council—causing further uncertainty about Iran's commitment to bring them to justice.

CHINA

Beijing's military modernization and military buildup is tilting the balance of power in the Taiwan Strait. Improved Chinese capabilities to threaten U.S. forces in the region.

• In 2004, China increased its ballistic missile forces deployed across from Taiwan and rolled out several new submarines.

• China continues to develop more robust, survivable nuclear-armed missiles as well as conventional capabilities for use in a regional conflict.

Taiwan continues to promote constitutional reform and other attempts to strengthen local identity. Beijing judges these moves to be a "timeline for independence". If Beijing decides that Taiwan is taking steps toward permanent separation that exceed Beijing's tolerance, we believe China is prepared to respond with various levels of force.

China is increasingly confident and active on the international stage, trying to ensure it has a voice on major international issues, secure access to natural resources, and counter what it sees as U.S. efforts to contain or encircle China.

New leadership under President Hu Jintao is facing an array of domestic challenges in 2005, such as the potential for a resurgence in inflation, increased dependence on exports, growing economic inequalities, increased awareness of individual rights, and popular expectations for the new leadership.

RUSSIA

The attitudes and actions of the so-called "siloviki"—the ex-KGB men that Putin has placed in positions of authority throughout the Russian government may be critical determinants of the course Putin will pursue in the year ahead.

• Perceived setbacks in Ukraine are likely to lead Putin to redouble his efforts to defend Russian interests abroad while balancing cooperation with the West. Russia's most immediate security threat is terrorism, and counterterrorism cooperation undoubtedly will continue.

• Putin publicly acknowledges a role for outside powers to play in the CIS, for example, but we believe he is nevertheless concerned about further encroachment by the U.S. and NATO into the region.

• Moscow worries that separatism inside Russia and radical Islamic movements beyond their borders might threaten stability in Southern Russia. Chechen extremists have increasingly turned to terrorist operations in response to Moscow's successes in Chechnya, and it is reasonable to predict that they will carry out attacks against civilian or military targets elsewhere in Russia in 2005.

Budget increases will help Russia create a professional military by replacing conscripts with volunteer servicemen and focus on maintaining, modernizing and extending the operational life of its strategic weapons systems, including its nuclear missile force.

• Russia remains an important source of weapons technology, materials and components for other nations. The vulnerability of Russian WMD materials and technology to theft or diversion is a continuing concern.

POTENTIAL AREAS FOR INSTABILITY

Mr. Chairman, in the Middle East, the election of Palestinian President Mahmud Abbas, nevertheless, marks an important step and Abbas has made it clear that negotiating a peace deal with Israel is a high priority. There nevertheless are hurdles ahead.

• Redlines must be resolved while Palestinian leaders try to rebuild damaged PA infrastructure and governing institutions, especially the security forces, the legislature, and the judiciary.

• Terrorist groups, some of who benefit from funding from outside sources, could step up attacks to derail peace and progress.

AFRICA

In Africa, chronic instability will continue to hamper counter-terrorism efforts and pose heavy humanitarian and peacekeeping burdens.

• In Nigeria, the military is struggling to contain militia groups in the oil-producing south and ethnic violence that frequently erupts throughout the country. Extremist groups are emerging from the country's Muslim population of about 65 million.

• In Sudan, the peace deal signed in January will result in de facto southern autonomy and may inspire rebels in provinces such as Darfur to press harder for a greater share of resources and power. Opportunities exist for Islamic extremists to reassert themselves in the North unless the central government stays unified.

• Unresolved disputes in the Horn of Africa—Africa's gateway to the Middle East—create vulnerability to foreign terrorist and extremist groups. Ethiopia and Eritrea still have a contested border, and armed factions in Somalia indicate they will fight the authority of a new transitional government.

LATIN AMERICA

In Latin America, the region is entering a major electoral cycle in 2006, when Brazil, Colombia, Costa Rica, Ecuador, Mexico, Nicaragua, Peru, and Venezuela hold presidential elections. Several key countries in the hemisphere are potential flashpoints in 2005.

• In Venezuela, Chavez is consolidating his power by using technically legal tactics to target his opponents and meddling in the region supported by Castro.

• In Colombia, progress against counternarcotics and terrorism under President Uribe's successful leadership, may be affected by the election.

• The outlook is very cloudy for legitimate, timely elections in November 2005 in Haiti—even with substantial international support.

• Campaigning for the 2006 presidential election in Mexico is likely to stall progress on fiscal, labor, and energy reforms.

In Cuba, Castro's hold on power remains firm, but a bad fall last October has rekindled speculation about his declining health and succession scenarios.

SOUTHEAST ASIA

In Southeast Asia, three countries bear close watching.

• In Indonesia, President Yudhoyono has moved swiftly to crackdown on corruption. Reinvigorating the economy, burdened by the costs of recovery in tsunami-damaged areas, will likely be affected by continuing deep-seated ethnic and political turmoil exploitable by terrorists.

• In the Philippines, Manila is struggling with prolonged Islamic and Communist rebellions. The presence of Jemaah Islamiyah (JI) terrorists seeking safe haven and training basses adds volatility and capability to terrorist groups already in place.

• Thailand is plagued with an increasingly volatile Muslim. separatist threat in its southeastern provinces, and the risk of escalation remains high.

Chairman ROBERTS. We thank you, Mr. Director, for a very comprehensive statement.

Director Mueller.

STATEMENT OF THE HONORABLE ROBERT MUELLER, DIRECTOR, FEDERAL BUREAU OF INVESTIGATION

Director MUELLER. Good morning, Mr. Chairman. Thank you. Thank you, Mr. Chairman and Senator Rockefeller and the Members of the Committee. I appreciate this opportunity to discuss our current view of threats to the United States and the FBI's efforts to address these threats.

Mr. Chairman, over the past year, through unprecedented cooperation, particularly with our other Federal agencies, but most particularly with State and local law enforcement, and with enhanced intelligence capabilities, we have achieved considerable victories against national security and criminal threats facing the United States.

However, at the same time, I must also report that these threats continue to evolve and to pose new challenges to the FBI and to our partners. It remains the FBI's overriding priority to detect and prevent terrorist attacks. And the threat posed by international terrorism, and in particular from al-Qa'ida and from related groups, continues to be the gravest threat that we face.

In 2004, we learned that terrorist cell members had conducted detailed surveillance of financial targets in New York, Washington, DC and New Jersey. In response to this threat and in coordination with the Department of Homeland Security, the threat level was raised. And we mobilized a substantial contingent of agents and analysts to review the massive amount of information connected with the attack planning and to uncover any additional information that would give us insight into that plot.

Later in the year, we received information suggesting that there would be an attack. There was an attack being planned, possibly timed to coincide with the period before the 2004 Presidential election.

To counter that threat, the FBI created a task force in May 2004, and with thousands of FBI personnel working together with hundreds of individuals from other agencies—Federal, State and local—we brought to bear every possible resource in an effort to identify the operatives and to disrupt the attack plan.

As part of the initiatives of this task force, field offices conducted a thorough canvas of all of our counterterrorism investigations, as well as all of our sources—not only counterterrorism sources, but other sources—in an effort to develop any further information that could help us find these individuals.

During the 7 months that the task force was up and running, we also checked every substantive lead provided in the threat intelligence. It was indeed an extraordinary effort, and while we may never know if an operation was indeed being planned, I am certain that our response to the threat played an integral role in disrupting any operational plans that may have been under way.

Mr. Chairman, since we last spoke, the FBI has identified various extremists located throughout the United States and is monitoring their activities. My prepared statement sets forth a number of instances in which we have taken legal action against individuals engaged in terrorism-related activities in Virginia, Minneapolis and New York. Although these efforts have made us safer, they are also a sobering reminder of the threat we continue to face.

There are three areas that cause us the greatest concern. First is the threat from covert al-Qa'ida operatives inside the United States who have the intention to facilitate or to conduct an attack. Finding them is the top priority for the FBI, but it is also one of our most difficult challenges. The very nature of a covert operative, trained not to raise suspicion and to appear benign, is what makes their detection so difficult.

Whether we are talking about a true sleeper operative who has been in place for years, waiting to be activated to conduct an attack, or a recently deployed operative who has entered the United States to facilitate or to conduct an attack, we are continuously adapting our methods to reflect newly received intelligence and to

ensure we are as proactive and as targeted as we can be in detecting their presence.

Second, we are also extremely concerned with the growing body of sensitive reporting that continues to show al-Qa'ida's clear intention to obtain, and to ultimately use, some form of chemical, biological, radiological or nuclear material in its attacks against the United States.

While we still assess that a mass casualty attack using relatively low-tech methods will be their most likely approach, we are concerned that they are seeking weapons of mass destruction, including chemical weapons, so-called dirty bombs or some form of biological agent such as anthrax.

Third, we remain concerned about the potential for al-Qa'ida to leverage extremist groups with peripheral or historical connections to al-Qa'ida, and particularly its ability to exploit radical American converts and other indigenous extremists. While we still believe that the most serious threat to the homeland originates from al-Qa'ida members located overseas, the bombings in Madrid last March have heightened our concern regarding the possible role that indigenous Islamic extremists already in the United States may play in future terrorist plots.

We are also concerned about the possible role that peripheral groups with a significant presence in the United States may play, if called upon by members of al-Qa'ida to assist them with attack planning or logistical support. The potential recruitment of radicalized American Muslim converts continues to be a concern and poses an increasingly challenging issue. The process of recruitment can be subtle, and many times self-initiated. And radicalization tends to occur over a long period of time and under very many different circumstances.

Efforts by extremists to obtain training inside the United States is also an ongoing concern. Although there are multiple reports and ongoing investigations associated with paramilitary training activities, I would suspect that extremists nationwide, the majority of these cases involve small groups of like-minded individuals who are inspired by the jihadist rhetoric found in radical mosques or in prison proselytizing or on the Internet.

Fortunately, the recent amendment to Title 18 adding a provision prohibiting individuals from receiving military-type training from a designated foreign terrorist organization makes it possible now to prosecute individuals who participate or assist individuals in receiving this type of training.

Mr. Chairman, al-Qa'ida and the groups that support it are still the most lethal threat we face today. However, other terrorist groups that have a presence in the United States require careful monitoring.

It is the FBI's assessment at this time that there is a limited threat of a coordinated terrorist attack in the United States from Palestinian terrorist organizations such as Hamas and the Palestine Islamic Jihad, and the al-Aqsa Martyrs Brigade. These groups have maintained a longstanding policy of focusing their attacks on Israeli targets in Israel and the Palestinian territories. We believe that the primary interest of Palestinian terrorist groups in

the United States remains the raising of funds to support their regional goals.

We are committed to cutting off the flow of these funds from the United States to Palestinian terrorist organizations. As an example of this effort, the former leadership of the Holy Land for Relief and Development, a Hamas front organization, was indicted this past year. And in another case, the Elashi brothers, who owned and ran InfoCom, another Hamas front organization, were prosecuted and convicted.

Of all the Palestinian groups, Hamas has the largest presence in the United States, with a strong infrastructure primarily focused on fundraising, propaganda for the Palestinian cause and proselytizing. Although it would be a major strategic shift for Hamas, its United States network is theoretically capable of facilitating acts of terrorism in the United States.

And like Hamas, but on a much smaller scale, the United States-based Palestine Islamic Jihad members and supporters are primarily engaged in fundraising, propaganda and proselytizing activities. In 2003, the Palestine Islamic Jihad, or PIJ, activities and capabilities in the United States were severely undercut by the arrests of the PIJ leader Sami al-Arian and his lieutenants. And there have been two additional arrests of suspected PIJ activists on charges unrelated to terrorism, which I believe are set forth in my accompanying statement.

Currently, the most likely threat of a terrorist attack from Palestinian groups in the United States—in the United States homeland—is from a lone-wolf scenario. In this scenario, a terrorist attack would be perpetrated by one or more individuals who may embrace the ideology of a Palestinian terrorist group, but act without assistance or approval of any established group.

And then, the Lebanese Hizbollah retains the capability to strike in the United States, although we have no credible information to indicate that United States-based Hizbollah members have plans to attack American interests within the United States or, for that matter, abroad.

I might add in 2004 we had successes in uncovering individuals providing material support to Hizbollah, many of those individuals involved in various criminal schemes to provide the monies that could be sent to Lebanon, to the coffers of Hizbollah.

Mr. Chairman, while the national attention is focused on the substantial threat posed by international terrorists to the homeland, the FBI must also dedicate resources to defeating a number of other threats, as detailed in my prepared statement—for example, domestic terrorists, motivated by a number of political or social agendas, including white supremacists, black separatists, animal rights/environmental terrorists, anarchists, anti-abortion extremists and self-styled militia groups; foreign intelligence activity, often using non-traditional collectors such as students and business visitors, targeting WMD information and technology, penetration of the United States government and compromise of critical, national assets.

There is the cyber threat from foreign governments, from terrorist groups and from hackers with the ability and the desire to utilize computers for illegal and harmful purposes.

And finally, there are the continuing threats posed to the fabric of our society by organized crime, human smuggling and trafficking, violent gangs, public corruption, civil rights violations, crimes against children and corporate fraud.

Mr. Chairman, in combating all these threats, from international terrorists to child predators, the FBI must effectively collect, analyze and share intelligence. As a result, over the past year we have continued to strengthen the FBI's enterprise-wide intelligence program. It began in 2001, with a dedicated analysis section in the Counterterrorism Division.

In 2002, we created the Office of Intelligence in the Counterterrorism Division. That structure has enhanced our capability significantly for purposes of our counterterrorism operations as well as the counterterrorism operations of our partners.

In 2003, we extended this concept across all FBI programs—criminal, cyber, counterterrorism and counterintelligence—and unified intelligence authorities under a new FBI Office of Intelligence, led by an Executive Assistant Director. The Office of Intelligence has adopted the intelligence community's best practices to direct all of our FBI intelligence activities. Congress and the 9/11 Commission reviewed these efforts, and provided recommendations to strengthen our capabilities.

In the last years, in intelligence reform legislation, alluded to by Senator Rockefeller, Congress directed us to create the Directorate of Intelligence—a dedicated national intelligence workforce within the FBI—and we are doing so. This workforce consists of intelligence analysts, language analysts, physical surveillance specialists and special agents who can pursue an entire career in intelligence.

This integrated intelligence service leverages the core strengths of the law enforcement community, such as reliability of sources and fact-based analysis, while ensuring that no walls exist between collectors, analysts and those who must act upon the intelligence information.

The Directorate also benefits from the strong FBI history of joint operations by unifying FBI intelligence professionals and integrating all partners, but most particularly, State, local and tribal law enforcement into our intelligence structures.

Mr. Chairman, my prepared statement provides additional information about the Directorate of Intelligence and the many steps that the Bureau has taken to expand and to strengthen its intelligence capabilities.

We continue to make progress, but there is still much work to do. We do not underestimate the challenges we face, but we are confident in our strategy and in our plans to protect the American people.

I again would like to thank you and the Committee for your support, and I look forward to working with you and the staff in the months—and hopefully the years—ahead. And I'm happy to answer any questions that you might have.

Thank you, sir.

[The prepared statement of Director Mueller follows:]

PREPARED STATEMENT OF HON. ROBERT S. MUELLER, III, DIRECTOR, FEDERAL BUREAU OF INVESTIGATION

Good afternoon, Mr. Chairman, Senator Rockefeller, and Members of the Committee. I appreciate this opportunity to discuss our current view of threats to the United States and the FBI's efforts to address them.

Before I begin, I would like to take a moment to thank all of our partners in the Law Enforcement and Intelligence Communities. They have shared their information and expertise, and in many cases worked side-by-side with us, and together we made great progress over the past year to protect our Nation and our communities from terrorism and crime.

I would also like to thank the men and women of the FBI for continuing to embrace our changing mission, for working to enhance our intelligence capabilities, for adapting to new technologies and new ways of doing things, and for doing all of this without ever pausing in our forward push to protect this country from active threats.

Mr. Chairman, over the past year, through unprecedented cooperation, enhanced intelligence capabilities, and continued unwavering commitment to protect the American people, we have achieved considerable victories against national security and criminal threats facing the U.S. However, I must also report that these threats continue to evolve and to pose new challenges to the FBI and our partners.

It remains the FBI's overriding priority to predict and prevent terrorist attacks. The threat posed by international terrorism, and in particular from al Qa'ida and related groups, continues to be the gravest we face.

AL-QA'IDA AND RELATED TERRORIST GROUPS

In 2004, our efforts in the War on Terrorism grew more intelligence-driven, more coordinated, and produced many tangible results.

In 2004 we learned that operatives had conducted detailed surveillance of financial targets in New York, Washington DC, and New Jersey. In response to this threat, in coordination with DHS, the threat level was raised from yellow to orange for the cities referenced in the threat and we mobilized a large contingent of analysts and agents to review the massive amount of information connected with the attack planning, and to uncover any additional information that would give us insight into the plot.

Previously, in the Spring of 2004, our allies in the United Kingdom arrested a group of terrorists who were plotting an imminent attack inside the UK. In response, we immediately formed a task force of analysts and agents to determine if there was a U.S. nexus to the plot or if any of the UK subjects had links to individuals in the U.S.

Later in the year, we received information suggesting that there was an attack being planned—possibly timed to coincide with the 2004 Presidential Election. To counter the threat, the FBI created the 2004 Threat Task Force in May 2004. With thousands of FBI personnel, supported by individuals from outside agencies, it was the largest task force created since 9/11, and it brought to bear every possible resource in an effort to identify the operatives and disrupt the attack plan.

As part of the Task Force's initiatives, field offices conducted a thorough canvass of all counterterrorism investigations and FBI sources to develop any further information that could help us find these individuals. During the 7 months the task force was up and running, we also checked every tangible lead provided in the threat intelligence. It was an extraordinary effort and while we may never know if an operation was indeed being planned, I am certain that the FBI's tremendous response to the threat played an integral role in disrupting any operational plans that may have been underway.

Mr. Chairman, since we last spoke, the FBI has identified various extremists located throughout the U.S. and is monitoring their activities. Although these efforts have made us safer, they are also a sobering reminder of the threat we continue to face.

• In Virginia, Mohammed Ali al-Timimi, the spiritual leader of the Virginia Jihad training group disrupted last year, was indicted for his involvement in the recruitment of U.S. citizens for extremist training and jihad preparation. Al-Timimi, the primary lecturer at a northern Virginia Islamic center, preached jihad to a small core group of followers, provided them paramilitary training and facilitated their travel to Pakistan in the days after September 11th to attend Lashkar-e-Taiba training camp in preparation to fight the United States in Afghanistan.

• In Minneapolis, we arrested Mohamad Kamal El-Zahabi, a Lebanese citizen who admitted to serving in Afghanistan and Chechnya as a sniper and to providing sniper training at Khalden camp in Afghanistan and in Lebanon in the 1990s. We

first learned of El-Zahabi during our investigation of Boston-based Sunni extremists Ra'ed Hijazi, convicted for his role in the Millennium plot in Jordan, and Bassain Kanj, who was killed in a plot to overthrow the Lebanese government in 2000.

• In New York, Yassin Muhiddin Aref was arrested on money laundering charges connected to a possible terrorist plot to kill a Pakistani diplomat.

Unfortunately, in spite of these accomplishments, al-Qa'ida continues to adapt and move forward with its desire to attack the United States using any means at its disposal. Their intent to attack us at home remains—and their resolve to destroy America has never faltered.

Al-Qa'ida's overall attack methodology has adapted and evolved to address the changes to their operating environment. While we still assess that a mass casualty attack using relatively low-tech methods will be their most likely approach, we are concerned that they are seeking weapons of mass destruction including chemical weapons, so-called "dirty bombs" or some type of biological agent such as anthrax.

Every day, personnel in our Counterterrorism Division and in 100 Joint Terrorism Task Forces around the country, work to determine where, when, and how the next attack will occur. The fact remains—America is awash in desirable targets—those that are symbolic like the U.S. Capitol and the White House—as well as the many infrastructure targets, like nuclear power plants, mass transit systems, bridges and tunnels, shipping and port facilities, financial centers, and airports—that if successfully hit, would cause both mass casualties and a crippling effect on our economy.

We continue to be concerned that U.S. transportation systems remain a key target. The attacks in Madrid last March show the devastation that a simple, low-tech operation can achieve and the resulting impact to the government and economy, which makes this type of attack in the U.S. particularly attractive to al-Qa'ida.

Another area we consider vulnerable and target rich is the energy sector, particularly nuclear power plants. Al-Qa'ida planner Khalid Sheikh Mohammed had nuclear power plants as part of his target set and we have no reason to believe that al-Qa'ida has reconsidered.

Looking ahead, there are three areas that cause us the greatest concern.

First is the threat from covert operatives who may be inside the U.S. who have the intention to facilitate or conduct an attack. Finding them is a top priority for the FBI, but it is also one of the most difficult challenges. The very nature of a covert operative—trained to not raise suspicion and to appear benign—is what makes their detection so difficult.

Mr. Chairman, while we are proud of our accomplishments this year and the additional insight we have gained into al-Qa'ida's activity, I remain very concerned about what we are not seeing.

Whether we are talking about a true sleeper operative who has been in place for years, waiting to be activated to conduct an attack or a recently deployed operative that has entered the U.S. to facilitate or conduct an attack, we are continuously adapting our methods to reflect newly-received intelligence and to ensure we are as proactive and as targeted as we can be in detecting their presence.

Second, because of al-Qa'ida's directed efforts this year to infiltrate covert operatives into the U.S., I am also very concerned with the growing body of sensitive reporting that continues to show al-Qa'ida's clear intention to obtain and ultimately use some form of chemical, biological, radiological, nuclear or high-energy explosives (CBRNE) material in its attacks against America.

Third, we remain concerned about the potential for al-Qa'ida to leverage extremist groups with peripheral or historical connections to al-Qa'ida, particularly its ability to exploit radical American converts and other indigenous extremists. While we still believe the most serious threat to the Homeland originates from al-Qa'ida members located overseas, the bombings in Madrid last March have heightened our concern regarding the possible role that indigenous Islamic extremists, already in the U.S., may play in future terrorist plots. Also of concern is the possible role that peripheral groups with a significant presence in the U.S. may play if called upon by members of al-Qa'ida to assist them with attack planning or logistical support.

The potential recruitment of radicalized American Muslim converts continues to be a concern and poses an increasingly challenging issue for the FBI because the process of recruitment is subtle and many times, self initiated and radicalization tends to occur over a long period of time and under many different circumstances.

As part of our continued efforts to identify populations that may be a target for extremist recruitment, the FBI has been involved in a coordinated effort between law enforcement and corrections personnel to combat the recruitment and radicalization of prison inmates. Prisons continue to be fertile ground for extremists who exploit both a prisoner's conversion to Islam while still in prison, as well as their socio-economic status and placement in the community upon their release.

Extremist recruitment at schools and universities inside the United States also poses a particularly difficult problem. Because the environment on campuses is so open and isolated, schools provide a particularly impressionable and captive audience for extremists to target.

Additionally, keeping in mind al-Qa'ida recruitment efforts occur primarily overseas, we are closely monitoring any possible methods for moving individuals to extremist-linked institutions overseas, specifically religious schools and mosques that have overt ties to al-Qa'ida or other terrorist organizations.

We are also concerned about the possibility that individuals who are members of groups previously considered to be peripheral to the current threat, could be convinced by more radical, external influences to take on a facilitation or even worse—an operational role—with little or no warning. Individual members of legitimate organizations, such Jama'at Tabligh, may be targeted by al-Qa'ida in an effort to exploit their networks and contacts here in the United States.

Efforts by extremists to obtain training inside the U.S. is also an ongoing concern. Although there are multiple reports and ongoing investigations associated with the paramilitary training activities of suspected extremists nationwide, the majority of these cases involve small groups of like-minded individuals who are inspired by the jihadist rhetoric experienced in radical mosques or prison proselytizing.

Fortunately, the recent amendment to Title 18 adding a provision whereby an individual knowingly receiving military-type training from a designated foreign terrorist organization is committing an offense, makes it possible to now prosecute individuals who participate or assist individuals in receiving this type of training.

Another area of concern is the recent merging of Iraqi jihadist leader Abu Mu'sab alZargawi with al-Qa'ida. Zarqawi has a demonstrated capability of directing external operations while maintaining his focus on Iraq as noted with the disrupted Jordan plot in April.

Another aspect of extremist activity in the U.S. is the extensive fundraising efforts by various terrorist groups. We continue to identify and block funding conduits, freeze assets of terrorists and those who support them, protect legitimate charities, and disrupt the movement of money through peripheral financial systems such as Hawalas.

As part of this effort, the FBI has engaged in extensive coordination with authorities of numerous foreign governments in terrorist financing matters, leading to joint investigative efforts throughout the world. The FBI's participation in a U.S.-Saudi Arabia Joint Terrorism Task Force, the U.S.-Swiss Terrorism Financing Task Force and the International Working Group on Terrorist Financing has enhanced cooperation between these agencies and the U.S. and allowed the FBI unprecedented access that has increased our understanding of these complex financing networks. Since 2002, we have provided terrorism financing training and technical assistance to liaison partners in almost 50 countries.

THE THREAT FROM OTHER INTERNATIONAL TERRORIST GROUPS

Mr. Chairman, al-Qa'ida and the groups that support it are still the most lethal threat we face today. However, other terrorist groups that have a presence in the U.S. require careful monitoring.

It is the FBI's assessment, at this time, that there is a limited threat of a coordinated terrorist attack in the U.S. from Palestinian terrorist organizations, such as HAMAS, the Palestine Islamic Jihad, and the al-Agsa Martyr's Brigade. These groups have maintained a longstanding policy of focusing their attacks on Israeli targets in Israel and the Palestinian territories. We believe that the primary interest of Palestinian terrorist groups in the U.S. remains the raising of funds to support their regional goals.

The FBI is committed to staunching the flow of funds from the U.S. to Palestinian terrorist organizations. As an example of this effort, the former leadership of the Holy Land for Relief and Development, a HAMAS front organization, was indicted this past year and convictions were won against the Elashi brothers who owned and ran Infocom, another HAMAS front organization.

Of all the Palestinian groups, HAMAS has the largest presence in the U.S. with a robust infrastructure, primarily focused on fundraising, propaganda for the Palestinian cause, and proselytizing. Although it would be a major strategic shift for HAMAS, its U.S. network is theoretically capable of facilitating acts of terrorism in the U.S.

Like HAMAS, but on a much smaller scale, U.S.-based Palestine Islamic Jihad members and supporters are primarily engaged in fundraising, propaganda and proselytizing activities. In 2003, the Palestine Islamic Jihad, or PIJ, activities and capabilities in the U.S. were severely undercut by the arrests of the U.S. PIJ leader,

Sami al-Arian, and three of his top lieutenants. There have also been two additional arrests of suspected PIJ activists on charges unrelated to terrorism. There has been no indication of a new U.S. PIJ leadership since the arrest of al-Axian.

Currently, the most likely threat of terrorist attacks from Palestinian groups to the U.S. homeland is from a "lone wolf 'scenario. In this scenario, a terrorist attack would be perpetrated by one or more individuals who may embrace the ideology of a Palestinian terrorist group, but act without assistance or approval of any established group.

Lebanese Hizballah retains the capability to strike in the U.S., although we have no credible information to indicate that US-based Hizballah members have plans to attack American interests within the U.S. or abroad. In 2004, we had some success in uncovering individuals providing material support to Hizballah.

• In Detroit, Mahmoud Youssef Kourani was indicted in the Eastern District of Michigan on one count of Conspiracy to Provide Material Support to Hizballah. Kourani was already in custody for entering the country illegally through Mexico and was involved in fundraising activities on behalf of Hizballah.

• Also in Detroit, Fawzi Assi was arrested in May of 2004 and was charged under the 1996 Antiterrorism and Effective Death Penalty Act for providing material support to Hizballah. Assi was initially arrested in 1998 after an outbound U.S. Customs search at the Detroit Metro Airport discovered night vision goggles, one thermal imaging scope and two Boeing Global Positioning System devices. Assi later fled the country after being released by the court on bail, but was later turned over to us in Lebanon to face U.S. criminal charges.

THE THREAT FROM DOMESTIC TERRORISM

While national attention is focused on the substantial threat posed by international terrorists to the homeland, law enforcement officials must also contend with an ongoing threat posed by domestic terrorists based and operating strictly within the U.S. Domestic terrorists motivated by a number of political or social agendas—including white supremacists, black separatists, animal rights/environmental terrorists, anarchists, anti-abortion extremists, and self-styled militia—continue to employ violence and criminal activity in furtherance of these agendas.

Animal rights and environmental extremists, operating under the umbrella of the Animal Liberation Front (ALF) and Earth Liberation Front (ELF) utilize a variety of tactics against their targets, including arson, sabotage/vandalism, theft of research animals, and the occasional use of explosive devices.

Serious incidents of animal rights/eco-terrorism decreased in 2004, a fact we attribute to a series of law enforcement successes that are likely deterring large-scale arsons and property destruction. Following a rash of serious incidents of animal rights/eco-terrorism, including a $50 million arson in San Diego and two bombing incidents in the San Francisco area, law enforcement authorities achieved several significant successes which have likely deterred additional terrorist activity. Despite these successes, we anticipate that animal rights extremism and eco-terrorism will continue to threaten certain segments of government and private industry, specifically in the areas of animal research and residential/commercial development.

The potential for violence by anarchists and other emerging revolutionary groups, such as the Anarchist Black Cross Federation (ABCF), will continue to be an issue for law enforcement. The stated goals of the ABCF are "the abolishment of prisons, the system of laws, and the Capitalist state." The ABCF believes in armed resistance to achieve a stateless and classless society. ABCF has continued to organize, recruit, and train anarchists in the tactical use of firearms.

U.S.-based black separatist groups follow radical variants of Islam, and in some cases express solidarity with al-Qa'ida and other international terrorist groups.

Incidents of organized white supremacist group violence decreased in 2004. This is due to several high profile law enforcement arrests over the last several years, as well as the continued fragmentation of white supremacist groups because of the deaths or the arrests of leaders. We judge that violence on the part of white supremacists remains an ongoing threat to government targets, Jewish individuals and establishments, and non-white ethnic groups.

However, the right-wing Patriot movement—consisting of militias, common law courts, tax protesters, and other anti-government extremists—remains a continuing threat in America today. Sporadic incidents resulting in direct clashes with law enforcement are possible and will most likely involve State and local law enforcement personnel, such as highway patrol officers and sheriff's deputies.

Potential violent anti-abortion extremists linked to terrorism ideologies or groups pose a current threat. The admiration of violent high-profile offenders by extremists

highlight continued concerns relating to potential or similar anti-abortion threat activity.

WMD PROLIFERATION AND OTHER FOREIGN INTELLIGENCE THREATS

Although the impact of terrorism is more immediate and highly visible, espionage and foreign intelligence activity are no less a threat to the U.S. national security. Many countries consider the U.S. to be their primary intelligence target; so long as the U.S. maintains its position in world affairs, it will continue to be targeted. As part of its reinvigorated and refocused foreign counterintelligence (FCI) program, the FBI has applied a more rigorous methodology to its efforts to assess and articulate the current threat environment.

One of the key elements of the FBI's *National Strategy for Counterintelligence* (adopted in August 2002) is the threat assessment. Over the past 2 years, the FBI has produced comprehensive threat assessments on several countries deemed to be of particular CI concern. The *National Strategy for Counterintelligence* identified five categories of foreign intelligence activity as being especially harmful to the U.S. national security. These five categories of activity are weighted in terms of importance, the in the following order:

- Proliferation of chemical, biological, radiological, nuclear, and high-energy explosives (CBRNE) information and technology:
- Penetration of the U.S. Intelligence Community (USIC)
- Penetration of U.S. Government entities and contractors
- Compromise of Critical National Assets (CNAs), defined as any information, policies, plans, technologies, or industries that, if stolen, modified, or manipulated by an adversary would seriously threaten U.S. national or economic security; and
- Conduct of clandestine foreign intelligence activities in the U.S.

Several countries have traditionally considered the U.S. to be their primary intelligence target, as well as an adversary or threat. This prioritization is manifested through their continued large and active intelligence presence in the U.S. and their aggressive targeting of U.S. persons, information and technology. Other countries, while not necessarily viewing the U.S. as an adversary or threat, seek information to help them compete economically, militarily, and politically in world affairs. As the current leader in all three areas, the U.S. becomes their primary target. For still other countries, rather than being an intelligence target, the U.S. represents an operating environment in which to conduct intelligence-related activities focused on their domestic security.

Some foreign countries are becoming increasingly sophisticated in their CI awareness, training and capabilities. Also of growing concern is the asymmetrical threat posed by certain intelligence services that supplement their collection capabilities in the U.S. by using non-traditional collectors. These collectors include students, delegations, business visitors, emigres, and retired intelligence officers who are collecting against targets of opportunity or responding to ad hoc requests from the intelligence services. Such non-traditional collectors pose a potential threat across the US, requiring a coordinated response by all FBI field offices.

The FBI does not foresee any significant changes in the official foreign intelligence presence in the U.S. over the next two to 3 years. However, in addition to using non-traditional collectors, several countries appear to be exploiting their military liaison officers, who are in the U.S. on overt, legitimate intelligence-sharing missions, to target and collect sensitive defense information that is outside the scope of their official access. Most difficult to identify and assess is the intelligence collection activity being directed and/or conducted by non-intelligence organizations, such as other foreign government agencies and/or foreign companies. The FBI sees this type of activity most frequently in the targeting and collection of CBRNE information and technology.

Another challenge the FBI will face is the tendency of some foreign intelligence services to leverage liaison relationships for intelligence collection purposes. U.S. Government representatives participating in international conferences and exchanges, or whose duties include routine liaison with foreign intelligence representatives, frequently report that their contacts engage in elicitation, sometimes to a surprisingly aggressive level.

The FBI expects to see a continued increase in the use of technology as an enabler for intelligence operations, such as contacting, tasking; and debriefing sources and agents in the US.

Over the near term, the priority collection targets for these countries will be:

- The effects of the recent 2004 U.S. elections on U.S. foreign and domestic policies;
- U.S. military actions in Iraq and Afghanistan;

- U.S. counterterrorism policy;
- U.S. dual use technologies; and
- U.S. policy vis-a-vis particular countries or regions of the world.

The FBI expects to see continued lobbying, political influence, and/or perception management activities by countries hoping to affect U.S. policy.

Many foreign intelligence services will also continue to exploit their presence in the U.S. to target and collect against third countries. Most will also engage in defensive intelligence activities, targeting their own expatriate and ethnic communities in the US, especially those groups deemed to be a threat to the current regime.

The FBI's *National Strategy for Counterintelligence* sets forth national priorities and strategic objectives as well as changes in management and organizational culture intended to redirect and significantly enhance the overall performance of the FBI's FCI program. Program objectives and outcomes include:

- Identify intelligence service objectives, officers, assets, and operations;
- Disrupt the operations of intelligence services; and
- Change the behavior of exploited institutions and individuals.

To that end, the FBI has identified five program strategies: Know the Domain; Understand the Threat; Engage in Strategic Partnerships; Conduct Sophisticated Operations; and Inform Policymakers.

During fiscal year 2004, the FBI FCI program accomplished the following:

- Six foreign intelligence officers and/or agents were arrested;
- 67 requests for persona non grata actions and visa denials were issued;
- 1,667 Intelligence Information Reports were disseminated.

In addition, the Asset Validation Review process was implemented in July 2002, and the FBI began providing mandatory asset validation training for Asset Coordinators in the field regarding procedures and policies. The FBI also implemented the Agents in Laboratories Initiative (AILI) in February 2003, through which FBI agents have been placed in Department of Energy nuclear weapons and science laboratories.

The FBI has also developed several strategic partnerships, to include the Regional CI Working Group (RCIWG) Initiative, which was established in October 2003 to implement the *National Strategy for Counterintelligence,* leverage the RCIWGs in tasking our USIC partners, address intelligence gaps, identify CI trends and priorities in the operational arena among USIC agencies at the field level, and ensure that all CI operational initiatives and projects across agencies are coordinated through the FBI.

Similarly, the National CI Working Group (NCIWG) was established and is led by the FBI and consists of other CI agency head-level representatives. The mission is to establish ongoing interagency planning discussions to better coordinate CI operations USIC-wide. Domain Task Forces are CI project level task forces led by the FBI, in vulnerabilities associated with at-risk national security projects, i.e., sensitive technologies, information, and research and development.

FBI field offices are developing "business alliances" to build executive-level relationships and foster threat and vulnerability information sharing, with private industries and academic institutions located within their territories having at-risk and sensitive national security and economic technologies, research and development projects.

Finally, the FBI has reinvigorated its CI training process. For example, field agents are trained in the key components of basic CI operations through an intensive 4-week Basic CI Operations course. Other advanced, highly specialized CI courses and seminars provide training to agents and analysts through a variety of innovative instructional methods and include inservices and conferences, the Interactive Multimedia Instruction and Simulation (IMIS) computer-based training program, and the FBI Intranet.

CYBER THREATS

The cyber-threat to the U.S. is serious and continues to expand rapidly the number of actors with both the ability and the desire to utilize computers for illegal and harmful purposes rises.

Cyber threats stems from both State actors, including foreign governments that use their vast resources to develop cyber technologies with which to attack our networks, and non-state actors such as terrorist groups and hackers that act independently of foreign governments. The increasing number of foreign governments and non-state actors exploiting U.S. computer networks is a major concern to the FBI and the Intelligence Community as a whole.

State actors continue to be a threat to both our national security as well as our economic security because they have the technical and financial resources to support

advanced network exploitation and attack. The greatest cyber threat is posed by countries that continue to openly conduct computer network attacks and exploitations on American systems.

Terrorists show a growing understanding of the critical role that information technology plays in the day-to-day operations of our economy and national security. Their recruitment efforts have expanded to include young people studying mathematics, computer science and engineering in an effort to move from the limited physical attacks to attacks against our technical systems.

Fortunately, the large majority of hackers do not have the resources or motivation to attack the U.S. critical information infrastructures. Most targets of the hacker are viewed as "challenges" to break into a system. These individuals do not introduce malicious code to the system, but usually leave their "cyber signature." Although a nuisance, the single hacker does not pose a great threat; however, the increasing volume of hacking activity worldwide does inadvertently disrupt networks, including that of the U.S. information infrastructures. Hackers that plant malicious code or upload bots that are designed to steal information are the main threats in this group. These individuals have the ability to take down a system or steal trade secrets, either of which can be devastating to a company or agency.

The growing number of hackers motivated by money is a cause for concern. If this pool of talent is utilized by terrorists, foreign governments or criminal organizations, the potential for a successful cyber attack on our critical infrastructures is greatly increased.

To combat these and other cyber threats, the FBI established a national cyber program with a Cyber Division at FBI Headquarters and dedicated cyber squads in the field offices. The program enables us to coordinate and facilitate investigations of those Federal criminal violations using the Internet, computer systems, or networks. It also helps us to build and maintain public/private alliances to maximize counterterrorism, counterintelligence, and law enforcement cyber response capabilities. We are also working to aggregate the technological and investigative expertise necessary to meet the challenges that lie ahead. We are recruiting and hiring individuals who possess degrees and experience in computer sciences, information systems, or related disciplines. We are looking for specialists who possess a bedrock of experience and a profound understanding of the cyber world.

CONVERGING CRIMINAL THREATS

It is increasingly the case that counterterrorism, counterintelligence, cyber, and criminal investigations are interrelated. There are rarely clear dividing lines that distinguish terrorist, counterintelligence, and criminal activity. Recognizing this trend toward convergence, the first priority of the FBI's Criminal Investigative Program is to leverage criminal investigative resources to enhance the FBI's Counterterrorism, Counterintelligence and Cyber programs.

Terrorists use criminal enterprises and criminal activities to support and fund terrorist organizations. The FBI's criminal investigations of these crimes and criminal enterprises, often in task forces in conjunction with other Federal, state, and local law enforcement, continue to develop invaluable intelligence, as well as to initiate investigations, which further identify the United States' vulnerability to attack and directly support the FBI's and the Intelligence Community's counterterrorism, counterintelligence, and cyber crime efforts.

One of the FBI's first investigations to utilize the material support of a terrorist organization statute evolved from a criminal investigation of Hizballah operators utilizing credit card scams, cigarette smuggling and loan fraud to support the purchase of dual use equipment for Hizballah procurement leaders in Lebanon. The FBI used the criminal RICO statute to fully neutralize this terrorist cell.

In combatting converging threats, the FBI's Criminal Program is placing greater emphasis on the collection, analysis, dissemination and effective use of intelligence, including intelligence derived from criminal investigations, including intelligence derived from human sources and the use of sophisticated investigative techniques. We are using intelligence to identify crime problems and trends, to conduct threat assessments, and to drive investigative efforts. Currently, we are aggressively pursuing intelligence collection and threat assessments on Organized Crime, Human Smuggling and Trafficking, Violent Gangs, Public Corruption, Civil Rights, and Middle Eastern Criminal Enterprises.

After CT, CI, and Cyber, the Criminal Investigative Program's other priorities in descending order are Criminal Intelligence, Public Corruption, Civil Rights, Violent Gangs, Criminal Enterprises, Corporate and Securities Fraud, Health Care Fraud, Mortgage Fraud, Major Financial Institution Fraud, and Crimes Against Children and other Violent Crimes.

Public Corruption

Public Corruption continues to pose the greatest threat to the integrity of all levels of government. Recent investigative efforts have been intensified to identify and convict Immigration, Department of State, and DMV officials illegally selling visas or other citizenship documents and drivers licenses to anyone with enough money. Their illegal activities potentially conceal the identity and purpose of terrorists and other criminals, facilitating their entry, travel, and operation without detection in the U.S. Other investigations have convicted numerous law enforcement officers, including those who formed criminal organizations involved in drug trafficking. Many major metropolitan areas in the U.S. have witnessed the indictment and conviction of corrupt public officials who betrayed the public trust for profit or personal gain. Over the last 2 years alone, the FBI has convicted more than 1050 corrupt government employees, including 177 Federal officials, 158 State officials, 360 local officials, and more than 365 police officers. In addition to pursuing criminal investigations against corrupt law enforcement officers, the FBI has initiated awareness and training efforts to deter corruption, such as "Project Integrity."

Civil Rights

During fiscal year 2004, the FBI initiated 1,744 civil rights investigations and obtained 154 convictions, focusing its efforts on Hate Crimes, Color of Law, and Involuntary Servitude and Slavery matters. The FBI and the United States depend on the support, cooperation and assistance of the Arab, Muslim and Sikh Communities in the United States to fight terrorism and to fight crime. These communities are entitled to the same civil rights of every citizen and person in the United States. The FBI has worked with these communities to ease their fears concerning the FBI's interest in securing their help in the fight against terrorism and to address the backlash of hate crimes directed against them following 9/11 and the war in Iraq. Since 9/11, more than 500 hate crime investigations have been initiated, where the victims were Arab, Muslim, Sikh, or perceived to be as such, resulting in more than 150 Federal and local prosecutions. During 2004, the FBI initiated 53 hate crime investigations where the victims were of Arab, Muslim, or Sikh descent or were perceived to be such. Thirteen of those cases resulted in criminal charges being filed by either State or Federal law enforcement authorities. Other groups also continue to be the victims of Hate Crimes, including African American and Jewish communities.

Human trafficking and modern day slavery are a worldwide crime and human rights problem, due to global, economic, and political factors. Approximately 17,000 victims each year are lured to the United States with false promises of good jobs and better lives and then forced to work under brutal and inhumane conditions. Many trafficking victims, including women and children, are forced to work in the sex industry, prison like factories, and migrant agricultural work.

Violent Gangs

Violent gangs are more organized, larger, more violent, and more widespread than ever before, and they pose a growing threat to the safety and security of Americans. The Department of Justice estimates there are approximately 30,000 gangs with more than 800,000 members in the U.S.

Our communities continue to experience devastating incidences of murder, drive-by shootings, and assaults by gangs mainly involved in the sale and distribution of illicit drugs. However, gang activity extends far beyond protection of turf. It impacts innocent citizens who have no connection or involvement with gangs, and it increasingly transcends municipal boundaries. Gang members travel from city to city, between states and, on occasion, between countries to commit their crimes.

In response, the FBI is implementing a coordinated, intelligence-driven National Gang Strategy to disrupt and dismantle gangs that pose the greatest threats to America's communities. In the past year, we have increased the number of Safe Street Task Forces from 78 to 107 and we are seeking to increase the number by an additional 10 to 20 percent in the coming year. We are also centralizing gang investigations at FBI Headquarters with a new $10 million National Gang Intelligence Center (NGIC). The NGIC will collect intelligence on gangs from across the U.S., analyze this intelligence, and disseminate it to help law enforcement authorities throughout the country plan and execute strategies to prevent further gang activity and violence.

The FBI has reclassified gang matters from "violent criminal offenders" to "criminal organizations and enterprises"—a higher priority area. The new classification also allows the U.S. Department of Justice to charge gang members under Federal racketeering statues which can result in stiffer prison sentences for convicted sub-

jects. This approach is similar to the successful strategy used by the FBI to dismantle traditional organized crime groups.

Under the National Gang Strategy, priority is given to efforts to disrupt and dismantle gangs that are national in their scope and exhibit significant connectivity and internal alliances. Among the first to be targeted is Mara Salvatrucha (MS–13), a violent gang which originated in Los Angeles comprised primarily of Central American immigrants. We have created a National Gang Task Force specifically to address MS–13.

Criminal Enterprises

Organized criminal enterprises operating in the U.S. and throughout the world pose increasing concerns for the international law enforcement and intelligence communities. Their skill in using international monetary systems to conduct and conceal their criminal activity, their use of State of the art communications encryption to further safeguard their illegal activity, and their transnational mobility increases the likelihood they will escape detection or otherwise cover their illegal activities with a cloak of legitimacy. Although the FBI prioritizes its efforts on criminal enterprises with possible connections to terrorist and counterintelligence activities, public corruption, human smuggling of Special Interest Aliens and women and children, or violent and pervasive racketeering activity, the impact from just one criminal activity alone, theft, is staggering. Annual property losses from cargo/high tech/retail theft is estimated at $30 billion, from vehicle theft $8 billion, from art/cultural heritage artifact theft $500 million, and from jewelry and gem theft $135 million. However, theft by criminal enterprises often represents a multifaceted threat. For example, Middle Eastern Criminal Enterprises involved in the organized theft and resale of infant formula pose not only an economic threat, but a public health threat to infants, and a potential source of material support to a terrorist organization.

The FBI is increasing its intelligence collection and assessment efforts on criminal enterprises, as well as its joint efforts with the intelligence and law enforcement services of other nations, to combat the criminal activities of the La Cosa Nostra, Italian, Russian, Balkan, Albanian, Asian, African, Middle Eastern, Colombian/South American and other criminal enterprises. The FBI/Hungarian National Bureau of Investigation Organized Crime Task Force in Budapest, Hungary, which is investigating a Russian Criminal Enterprise engaged in murder, extortion, prostitution, and other significant racketeering activity, represents an unprecedented cooperative effort between the FBI and the Hungarians.

Although new criminal enterprises continue to emerge, the LCN remains a formidable and ever changing criminal threat. This year, in just one criminal scheme, identified by the Federal Trade Commission as the largest consumer fraud investigated in the history of the United States, members of the Gambino LCN family were convicted for using pornographic websites and adult entertainment 1 800 numbers to defraud thousands of individuals of $750,000,000. Asian Criminal Enterprises also pose a continued threat, as exemplified by one which was dismantled earlier this year during a coordinated arrest operation with Canada, which resulted in the arrest of 36 subjects in Canada and 102 subjects in the U.S. for drug trafficking and money laundering. Millions of dollars and 21 firearms, including an AK 47 assault rifle and a sawed off shotgun were seized during the operation.

Corporate/Securities Fraud

Corporate fraud can cost Americans their jobs and rob them of hard-earned savings. It shakes the public's confidence in corporate America to its foundation. Since the initiation of the FBI Corporate Fraud Task Force in December 2001, there have been 480 indictments and 305 convictions of corporate executives and their associates. The FBI's efforts have also resulted in over $2 billion in restitutions, recoveries and fines, in addition to over $30 million in seizures and forfeitures. In the Enron, HealthSouth, Cendant Corporation, Credit Suisse First Boston, Computer Associates International, Worldcom, Imclone, Royal Ahold, Perigrine Systems, and America Online cases the FBI obtained 119 indictments/informations and 79 convictions. The former Chief Executive Officer (CEO) of Worldcom is on trial in New York and the former CEO of HealthSouth is on trial in Alabama. Several additional high profile trials are anticipated in the near future, to include the trial of Enron's former CEOs and Chief Accounting Officer anticipated to be scheduled for August or September 2005.

The FBI is currently pursuing 334 Corporate Fraud cases throughout the U.S. This is more than a 100 percent increase from fiscal year 2003. Eighteen of the pending cases involve losses to public investors which each exceed $1 billion. Unfortunately, the volume of cases has yet to reach a plateau, and the FBI continues to

open three to six new cases each month, each case averaging a loss exceeding $100 million.

Health Care Fraud

Americans' health care expenditures continue to climb at rates higher than inflation and will soon consume more than 17 percent of the Gross Domestic Product. It is estimated that health care fraud costs consumers, Medicare, Medicaid, and private insurers tens of billions of dollars each year in blatant fraud schemes in every sector of the industry. The FBI recently instituted the Out Patient Surgery and Pharmaceutical Fraud Initiatives to combat blatant fraud identified in those health care programs. During fiscal year 2004, the FBI had 2,468 pending health care fraud investigations, obtained 693 indictments and informations, 564 convictions or pre trial diversions, $1.05 billion in restitution, $543 million in fines, $28.8 million in seizures, $19.05 million in forfeitures and disrupted 186 and dismantled 105 criminal organizations.

Mortgage Fraud

The number of FBI mortgage fraud investigations, including major undercover operations, rose from 102 in fiscal year 2001 to approximately 550 in fiscal year 2004. This rise is expected to continue. During FYs 2001–2004 the FBI received over 17,000 mortgage fraud related Suspicious Activity Reports from federally insured financial institutions alone. The FBI worked with the Mortgage Bankers' Association (MBA), the National Notary Association (NNA), as well as FINCEN, the Department of Housing and Urban Development, and major mortgage lending institutions, to improve the reporting and detection of potential mortgage fraud.

Crimes Against Children / Violent Incident Crime

Of all violent crime, crimes against children and child prostitution are of particular concern. Over 300,000 children per year are forced into prostitution. The FBI's Lost Innocence, Child Prostitution Initiative, has opened 13 cases in 11 field offices, emphasizing the use of sophisticated investigative techniques, to obtain 135 arrests/locates, 3 complaints, 13 indictments/informations, 11 convictions/pre trial diversions, and 4 child locates. Major violent crime incidents, such as sniper murders, serial killings and child abductions can paralyze whole communities and require the cooperative efforts of the FBI and local, State and other Federal law enforcement agencies. The FBI also continues to address the 6,218 bank robberies, resulting in 153 injuries, and 15 deaths, that occurred within the first 10 months of 2004, albeit with a greater reliance on other agencies and a lesser use of its own resources where possible.

ENHANCING THE FBI'S CAPABILITIES

Mr. Chairman, you will notice that our accomplishments over the past year consistently have two things in common, the effective collection and use of intelligence and inter-agency cooperation. The improvements that made these accomplishments possible result from the continued efforts of the men and women of the FBI to implement a plan that fundamentally transforms our agency and enhances our ability to predict and prevent terrorism.

Intelligence

As set forth above, threat information crosses both internal and external organizational boundaries. Counterterrorism efforts must draw from, and contribute to, counterintelligence, cyber and criminal programs. In order to most effectively address all threats, we are continuing to strengthen the FBI's enterprise-wide intelligence program.

We began in 2001 with a dedicated analysis section in the Counterterrorism Division and, in 2002, we created an Office of Intelligence in the Counterterrorism Division. The structure and capability significantly enhanced our CT operations and those of our partners. In 2003, we extended this concept across all FBI programs—Criminal Cyber, Counterterrorism and Counterintelligence—and unified intelligence authorities under a new FBI Office of Intelligence led by an Executive Assistant Director. The Office of Intelligence adopted Intelligence Community best practices to direct all FBI intelligence activities. Congress and the 9/11 Commission reviewed these efforts and provided recommendations to further strengthen the FBI's intelligence capability.

The newly established Directorate of Intelligence is the dedicated national security workforce that the Congress established within the FBI. It comprises a dedicated Headquarters element and embedded intelligence entities in each FBI field office called Field Intelligence Groups (FIGs). The FIGs are central to the integration

of the intelligence cycle into field operations. The FIGS include Special Agents, Intelligence Analysts, Language Specialists, and Surveillance Specialists, as well as officers and analysts from other intelligence and law enforcement agencies. They are responsible for coordinating, managing, and executing all of the functions of the intelligence cycle and have significantly improved the FBI's intelligence capability. This integrated intelligence service leverages the core strengths of the law enforcement culture—such as reliability of sources and fact-based analysis—while ensuring that no walls exist between collectors, analysts and those who must act upon intelligence information. The Directorate also benefits from the strong FBI history of joint operations by unifying FBI intelligence professional and integrating all partners, particularly state, local, and tribal law enforcement, into our intelligence structures.

The central mission of the Directorate is to optimally position the FBI to meet current and emerging national security and criminal threats by: (1) assuring that the FBI proactively targets threats to the US, inhibiting them and dissuading them before they become crimes; (2) providing useful, appropriate and timely information and analysis to the national security, homeland security, and law enforcement communities; and (3) building and-sustaining FBI-wide intelligence policies and capabilities.

In 2004, we made substantial progress to expand and strengthen our intelligence workforce. For the first time, the FBI offered recruitment bonuses for Intelligence Analysts. As a result of these and other efforts, the FBI received over 80,000 applications and hired over 650 Intelligence Analysts.

We built on the College of Analytic Studies, created in October 2001, with the addition of two new courses based on intelligence community best practices: ACES 1.0, a new basis intelligence analytic course, and ACES 1.5, a course for experienced, on-board analysts that provides information on the latest analytic resources and techniques. To ensure a consistent level of knowledge across the workforce on intelligence concepts and processes, ACES Training is now mandatory for all FBI Intelligence Analysts. We have increased our training expertise and capacity and are on track to deliver basic training to 1,000 Intelligence Analysts by December 2005. In addition, we have incorporated intelligence training into New Agents class, including a joint exercise with Intelligence Analysts and joint evening seminars.

The Intelligence Analyst career path, with multiple work roles and cross-training requirements not only provides career development opportunities, it also creates a workforce with the agility and flexibility needed to respond to the changing threat environment.

In addition, we implemented several initiatives to enhance the analyst career path and improve retention. We extended the promotion potential for analysts in the field from GS–12 to GS–14. We created an Intelligence Analyst Advisory Board, leveraging the strong FBI culture of creating advisory groups to provide advocacy for specific career fields. At the same time we worked with Congress and were granted pay flexibilities, such that FBI intelligence professionals now can be compensated at a rate equal to that of their Intelligence Community peers. These and other initiatives have helped us to stabilize our attrition rate between 8 percent and 9 percent and FY05 statistics to date look promising.

We have also taken steps to strengthen the Special Agent component of our intelligence workforce. In March 2004 we established a new career path for Special Agents with three objectives. First, the career path gives all Agents experience in intelligence collection, analysis and dissemination. Second, the career path will give Agents an opportunity to develop specialized skills, experience and aptitudes in one of four areas: 1) Intelligence, 2) Counterterrorism/Counterintelligence, 3) Cyber or 4) Criminal. Third, it makes Intelligence Officer Certification a prerequisite for advancement to senior supervisory ranks. The Special Agent career path will produce a cadre of Agents who are proficient in both intelligence and law enforcement operations. This is key to achieving the full integration of law enforcement and intelligence operations.

To improve our foreign language capabilities, we have recruited and processed more than 50,000 translator applicants. These efforts have resulted in the addition of 778 new Contract Linguists (net gain of 493 after attrition) and 109 new Language Analysts (net gain of 34 after attrition). The FBI has increased its overall number of linguists by 67 percent, with the number of linguists in certain high priority languages increasing by 200 percent or more.

We have integrated management of the FBI's Foreign Language Program (FLP) into the Directorate of Intelligence. This integration fully aligns F13I foreign language and intelligence management activities and delivers a cross-cutting platform for future improvements across all program areas, including translation quality controls.

We also established the Language Services Translation Center (LSTC), a command and control structure at FBI Headquarters to ensure that our finite translator resource base of over 1,300 translators, distributed across 52 field offices, is strategically aligned with priorities set by our operational divisions on a national level.

We have built a secure network that allows us to efficiently route FISA audio collection to any FBI field office. This technology allows us to more effectively utilize our national translator base.

We now possess sufficient translation capability to promptly address all of our highest priority counterterrorism intelligence, often within 12 hours. Of the several hundred thousand hours of audio materials and several million pages of text collected in connection with counterterrorism investigations over the last 2 years, a nominal level of backlog exists only because of obscure languages or dialects.

We have instituted a national translation quality assurance program. Countervailing operational pressures, however, limit our ability to fully comply with instituted translation review procedures in those languages for which demand continues to outpace supply. In those languages for which we have already achieved excess translation capacity, e.g., Farsi, Pashto, and Vietnamese, 100 percent quality assurance compliance is expected by April 2005.

Translation backlogs continue to exist within our counterintelligence program. To target these deficiencies, we have implemented a highly successful workforce planning model which links field-wide workload measurements, trend analysis, and geopolitical indicators to our recruitment and applicant processing efforts.

In 2005, we plan to strengthen the integration of the entire intelligence cycle (requirements management; planning and direction; collection; processing and exploitation of collected information; analysis and production; and dissemination) into field office operations.

We will incorporate the recently developed new critical element entitled, "Intelligence," into the performance plans of all Special Agents and Supervisory Special Agents; this new element emphasizes participation in intelligence cycle functions, in particular human source development and contributions to intelligence production.

We will also establish "fly teams" of Agents with intelligence experience, Intelligence Analysts, Language Specialists, and Surveillance Specialists to travel to five field offices and provide hands-on guidance and training for the full integration of the intelligence cycle within the office.

Partnerships

Our ability to coordinate and communicate with other members of the Intelligence Community has never been better. Our face-to-face interaction with the National Counterterrorism Center and members of the CIA and DHS has positively impacted our ability to come together on a common problem and the results of the cooperation are evident. Case in point—during the election threat, analysts were able to meet daily to discuss assessments and develop theories that were fundamental to understanding the threat, and from those meetings, online forums were created to facilitate continued sharing of ideas and new intelligence finds—all from the desktop.

The FBI's Information Sharing Policy Group, chaired by the FBI's EAD—Intelligence, brings together the FBI entities that generate and disseminate law enforcement information and intelligence to implement the FBI's goal of sharing as much as possible consistent with security and privacy protections.

Within the Intelligence Community, the FBI has a two-level approach:

1. For those agencies that operate at the Top Secret-SCI level, we are investing in secure facilities for an FBI network (SCI On-Line, or SCION) that is linked to the DoD-based JWICS network used by CIA, NSA, and other national agencies.

2. For those agencies that operate at the Secret level, we have connected the FBI's internal electronic communications system to the DoD-based SIPRNET network that serves. As a result, all FBI Agents or analysts who need to communicate at the Secret-level with other agencies can do so from their desktop.

Within the law enforcement community, the FBI's National Information Sharing Strategy (HISS) is part of the DOJ Law Enforcement Information Sharing Program and builds upon the FBI Criminal Justice Information (CJIS) Services program.

1. The Law Enforcement National Data Exchange (N-DEx) will provide a nationwide capability to exchange data derived from incident and event reports. Data from incident and arrest reports—name, address, and non-specific crime characteristics—will be entered into a central repository to be queried against by future data submissions. The national scale of N-DEx will enable rapid coordination among all strata of law enforcement.

2. The Law Enforcement Regional Data Exchange (R-DEx) will enable the FBI to join participating Federal, state, tribal, and local law enforcement agencies in re-

gional fulltext information sharing systems under standard technical procedures and policy agreements.

3. The FBI makes national intelligence more readily available to state, tribal, and local law enforcement agencies through the Law Enforcement Online (LEO) network.

4. The Terrorist Screening Center (TSC) also leverages the CJIS backbone to provide realtime actionable intelligence to State and local law enforcement.

Information Technology

Recognizing that the ability to assemble, analyze and disseminate information both internally and with other intelligence and law enforcement agencies is essential to our success in the war on terrorism, the FBI has made modernization of its information technology (IT) a priority.

Under the centralized leadership of the Chief Information Officer (CIO), the FBI is now taking a coordinated, strategic approach to IT. We have a Strategic IT Plan, a baseline Enterprise Architecture, and a system for managing IT projects at each stage of their "life cycle" from planning and investment, through development and deployment, operation and maintenance, and disposal. This involves regular technical reviews to see if milestones are met.

The first two phases of the Trilogy IT modernization program have been completed. The FBI is now modernized with:

1. Deployment of a high-speed, secure network that enables personnel in FBI offices around the country to share data, including audio, video and image files.

2. More than 30,000 new desktop computers with modern software applications 3,700 printers, 1600 scanners, 465 servers and 1400 routers.

3. An IT infrastructure that provides for secure communication with our Intelligence Community partners.

The third phase of Trilogy, which includes the Virtual Case File (VCF) has not yet been completed. Plans for VCF have changed both in response to identified technical problems and because the FBI's refocused mission created requirements that did not exist when VCF was originally envisioned, such as requirements related to information sharing. Last June, after we determined that the product delivered did not meet our needs, we decided to move forward with a two-track action plan for VCF.

1. In accordance with this plan, we asked a new contractor to examine the latest working version of the VCF as well as available off-the-shelf software applications and those designed for other agencies, to determine the best combination to meet the FBI's needs. In many ways, the pace of technological innovation has overtaken our original vision for VCF, and there are now existing products to suit our purposes that did not exist when Trilogy began.

2. As we move forward, we will apply all that we have learned and leverage what we have already developed, including a critical interface to our existing data systems that will be a key component of our final solution.

Separate from the Trilogy Program, we have successfully developed and deployed a number of new investigative and information sharing capabilities.

The *Investigative Data Warehouse (IDW)* offers Agents and analysts alike the technology to perform link analysis, while also providing enhanced search and analytical tools. IDW provides FBI users with a single access point to more than 47 sources of counterterrorism data, including information from FBI files, other government agency data, and open source news feeds, that were previously available only through separate, stove-piped systems. Most of these users are with the Directorate of Intelligence, Counterterrorism or Counterintelligence Divisions. These users provide search and analysis services using the IDW for personnel throughout the Bureau.

The *FBI Automated Messaging System (FAMS)* began operations in December and now provides more than 300 users with the capability to send and receive critical organizational message traffic to any of the 40,000+ addresses on the Defense Messaging System (DMS). The FBI is the first civilian agency to operate a classified DMS.

The *FBI Intelligence Information Reports Dissemination System (FIDS)* is a web-based software application that allows all FBI personnel with access to the FBI's Intranet to create and disseminate standardized Intelligence Information Reports (IIRs) quickly and efficiently. FIDS allows the Directorate of Intelligence to automate and standardize IIR creation and dissemination functions.

CONCLUSION

Looking forward, we expect certain trends to continue. Our adversaries will keep evolving, national security and criminal threats will further converge, and old juris-

dictional boundaries will become less and less relevant. If we are to address these trends successfully, we must be willing and able to evolve ourselves. The FBI must continue to build our intelligence capabilities, including a strong intelligence workforce. We must continue hiring and training personnel with technical expertise and foreign language skills. We must continue to seek new ways to share information and collaborate with partners in the Intelligence and Law Enforcement Communities. Above all, we must be agile, and encourage creativity, innovation, and strategic thinking. If we do all of these things, I am confident that we will out-network, out-think, and ultimately defeat our adversaries.

Mr. Chairman, I thank you again for this opportunity. I look forward to working with this Committee as we continue our efforts to address threats to the U.S. I would be happy to take any questions you might have.

Chairman ROBERTS. Mr. Mueller, we thank you for your statement as well and thank you for the job you're doing, in a very difficult challenge in changing the mission of the FBI and still keeping the mission in regards to crime and in regards to law enforcement.

I would say to all Members that Ms. Rodley and Admiral Jacoby are here to answer questions. And so, Admiral Loy will give the last prepared statement.

And I neglected to tell all of you that each and every word of your testimony will be in the record and preserved for all time. And so, feel free to summarize your statements.

I apologize. That's not an admonition, that's just a statement.

Admiral Loy. And I'm not trying to pick on you.

STATEMENT OF ADMIRAL JAMES LOY, U.S. COAST GUARD, RET., DEPUTY SECRETARY, DEPARTMENT OF HOMELAND SECURITY

Admiral LOY. Thank you, Mr. Chairman. Good morning, Chairman Roberts and Vice Chairman Rockefeller and distinguished Members of the Committee. I'm pleased to have the chance to appear before you today to discuss the threats against the U.S. homeland, as well as some of the capabilities we've developed and must continue to develop to confront these threats.

That important link between the intelligence we process and the systems we develop in response cannot be understated. For every possible action we uncover, there must be an intentionally focused reaction designed to secure our homeland against that threat.

In so many areas of greatest concern, vulnerabilities we've identified, such as our transportation systems, particularly air travel, our border functions and our critical infrastructure, such as ports and energy facilities, we've made very real, measurable progress that has made our Nation more secure.

The topic of our hearing is very straightforward. What is the nature of the worldwide threat? And from the DHS perspective, I would make simply five, basic points.

First, the threat is unclear and complex, but enduring. The condition is not expected to change. We continue to note attempted entry into the U.S. by aliens who, according to intelligence, pose a threat to our homeland.

Second, we assess that al-Qa'ida continues to be the primary transnational threat group, although we are seeing the emergence of other threatening groups and gangs, like MS–13, that will also be destabilizing influences.

Third, we think we are most likely to be attacked with a vehicle-borne improvised explosive device, because that's the weapon of choice around the world. However, it remains very clear that our primary adversaries continue to seek weapons of mass effects with which they intend to strike us if they acquire them.

Fourth, at DHS we continue to make progress in acquiring analysts and improving our capabilities, just 2 years into our existence. However, we have not yet fully achieved the capability in people, facilities and technical capability we think is necessary to protect our homeland. We can, and we are doing the job, through extraordinary effort on the part of our intelligence professionals and through the collegial efforts of all of those at this table and many other agencies in the Federal sector.

And last, the intelligence community interaction with DHS has markedly improved over this past year and we continue to work toward full integration and interoperability. The aftermath of the Intelligence Reform Act is being treated as an opportunity to complete that work, to earn the respect of our colleagues as a full and deserving player in the intelligence community, and to allow that respect to serve as the foundation DHS needs to fulfill its responsibilities to secure our homeland.

Thankfully, we have not experienced another attack on our soil since September 11, 2001. But the rest of the world has not been so fortunate. If you ask the residents of Madrid or Beslan or Bali or Jakarta or many others, they will assure you that not only the threat, but also the harsh daily reality of terrorism is alive and well around the world.

We realize that an attack here could come in any form at any place on any timetable. Terrorist groups—even ones whose capabilities may have been weakened by arrests and interdictions worldwide—are patient, strategic and methodical in their operational planning. At home, we must prepare ourselves for any attack, from IEDs to weapons of mass destruction, from soft targets like malls to national icons.

Intelligence suggests that al-Qa'ida may have specific tendencies or certain intentions, both small- and large-scale. And our efforts must stay directed to this full range of threats. We must assume that they are assembling, or reassembling, the capabilities they don't currently have or those that have been taken from them. So our plan of action, like theirs, must be even more deliberate and even more enduring, and it is.

We have built new tools to help in each of the five strategic areas of operational emphasis in our department. Our charter runs from maximum domain awareness, if you will, through prevention and protection efforts to response and recovery planning. We have published an all-hazards, all-threats National Response Plan and its sister document, the National Incident Management System.

We have dramatically improved our technical ability to share information. Tools such as the Homeland Security Operations Center, the Homeland Security Information Network and the Homeland Security Advisory System are steps toward full capacity and capability. We know the end state we want to reach and we are methodically designing the path to get there.

We have greatly improved systems to keep track of persons who cross the border and we have begun to apply technology to monitor the border where there is no human presence. We're operating the US-VISIT Program to verify the identity of travelers and stop criminals and terrorists before they can enter our society.

We have signed Smart Border accords with our neighbors to the north and south, Canada and Mexico, to help the highly trained customs officers, border agents, Coast Guardsmen and many others who monitor and patrol our Nation's nearly 7,500 miles of land border and 95,000 miles of coastline and waterways.

We now require unprecedented scrutiny of high-risk travelers and flights landing in or flying over the United States, including requiring volumetric information on visas and passports and agreeing to share passenger data with our European allies. These are important strides to keep the doors of our country open to legitimate visitors, but firmly shut to terrorists.

We know that al-Qa'ida would like to impact our economy with attacks on our financial systems, our cyber networks and the vital elements of our global supply chain. So we've taken measures to secure cargo and protect the infrastructure that supports the free and safe movement of goods and people and money around the world.

We launched the Container Security Initiative to target and screen high-risk cargo before it reaches our shores. And today we operate that program alongside our allies in 34 ports around the world in 22 different countries with a growth posture scheduled for 2005 and on into 2006. We are in the process of finalizing, with the input from private sector stakeholders as well as many others, a national cargo security strategy.

We included a special section on cyber security in the newly released National Response Plan to enhance governmentwide collaboration and coordination to prevent an attack on the backbone of our electronic economy.

And most important, we've been careful to consider the economic impacts and the privacy implications of any additional security efforts, and worked to ensure that added protections do not detract from our competitiveness or from our way of life.

In ways large and small, seen and unseen, with advanced technologies and additional vigilance, with the help of countless agencies and allies at every level of government, in the private sector and throughout the world, we have made it harder for terrorists to attack our country, more difficult for them to defeat our systems and reduce large gaps they once saw in our security posture.

As the President has said, we are safer than ever before, but we are still not safe enough. This experiment called DHS is astonishingly complex and some dimensions of the challenge are further along than others. That's the nature of culture and transformational change. I'm proud to hand over a 2-year-old department with a solid foundation and a solid sense of direction to our incoming leadership team.

I'm deeply appreciative of the support, constructive criticism and the resources that have come our way over the past 2 years from the Congress. This Committee's continued focus and review must remain our Nation's conscience until we get this work accomplished.

Last night, I spoke to a group of 400 young people—high school people—in a program geared to encouraging public service. I promised them that we would do all we could to lighten their burden when it's their turn on watch. And we can only meet that promise when our national intelligence capability is sound, inclusive, whole. Anything short of that is simply unsatisfactory.

Thank you, Mr. Chairman. I'll happily answer your questions.

[The prepared statement of Admiral Loy follows:]

PREPARED STATEMENT OF ADMIRAL JAMES LOY, DEPUTY SECRETARY, U.S. DEPARTMENT OF HOMELAND SECURITY

Good morning Chairman Roberts, Vice Chairman Rockefeller, and distinguished Members of the Committee. I am privileged to appear before you today to discuss the primary threats currently facing the United States homeland, as well as their probability, immediacy, and severity.

Most current threats to the homeland continue to be directed by al-Qaida and its affiliated elements within the broader Sunni extremist movement. Despite the successes the United States and our coalition partners have had against al-Qaida and other extremists, al-Qaida leaders and operational planners continue to think about—if not actively plot—the next dramatic attack in the United States. We believe that attacking the homeland remains at the top of al-Qaida's operational priority list, despite the fact that more than 3 years have passed since September 11, 2001. We judge that al-Qaida continues to view the homeland as an attractive target for a variety reasons, and that the next dramatic attack will attempt to replicate the 9/11 "model" of multiple attacks against geographically distant and symbolic targets that cause unprecedented economic damage, mass casualties, and physical destruction. While al-Qaida and its affiliated elements currently appear more capable of attacking United States interests outside of the homeland, we believe that their intent remains strong for attempting another major operation here.

While there are other transnational terrorist groups that possess noteworthy capabilities to conduct attacks against United States interests, we currently do not believe these groups are ready for or oriented toward conducting attacks inside the homeland. However, there is a legitimate threat posed by groups and persons who are present in the country today (not necessarily connected to transnational terrorist groups), including multi-national gangs and domestic groups that engage in violence to achieve political and economic goals. These groups range from single-issue groups such as the Earth Liberation Front to violent criminal gangs like MS–13 to right-wing or neo-Nazi groups to "lone-wolf' threats. Additionally, the threat from criminal groups and persons who engage in criminal enterprise that supports or contributes to terrorism and which has homeland security implications remains of concern. Examples of such activity include narcotics trafficking, money laundering, people smuggling, contraband smuggling, illegal arms transfers, illegal technology transfers, currency counterfeiting, document forgery, and false identity provision. However, none of these threats currently rises to the level of threat posed by al-Qaida and its affiliates.

While there is no single "crystal ball" that allows intelligence analysts to perfectly determine which terrorist threats are the most probable, we believe the al-Qaida and affiliated extremist threat remains the most likely in the near term. The strategic intent of al-Qaida's remaining leaders and planners to attempt another dramatic homeland attack is clear. What is less clear are al-Qaida's current operational capabilities to execute such an attack. Though al-Qaida's current capabilities for dramatic attacks inside the United States might seem reduced, we also assess, based on past activity, that a1-Qaida is patient, deliberate, and methodical in operational planning for major attacks. Al-Qaida operates on a very long timeline.

Thus, the probability of an attack in the United States is assessed to be high, but very much conditional and circumstantial. We believe that while several attacks may have been considered inside the U.S. since 9/11, and some moved forward beyond initial planning, none of these plots was ever successfully executed due to the attackers' operational limitations and the heightened intelligence and security measures employed since that time.

The cyber risk from various types of malicious actors is more significant than previously understood, and could be used to increase the impact of a physical attack by disrupting emergency communications.

The National Intelligence Council released last year its first National Intelligence Estimate (NIE) for worldwide cyber security since 9/11, and the DHS/National

Cyber Security Division's law enforcement and intelligence branch participated in that assessment. It assessed the cyber threat, and the result showed a significant capability and threat from various actors.

Adding to our concern over the possibility of the next al-Qaida attack is the potential threat of individuals inspired by al-Qaida and its affiliates who are not in any way directly connected to the al-Qaida core. In early 2004, several individuals in the United Kingdom attempted to conduct attacks there, but none of these individuals was considered an active al-Qaida member. This and other examples of similar activity in Europe demonstrate how individuals or small groups, who previously had provided only financial or logistical support to Islamic extremist activities, themselves attempted to transition into active operational roles.

The key locales that we currently judge as being at risk for attack by al-Qaida and affiliated terrorist organizations include key person and large group assemblages, major events as judged by the Department of Homeland Security (DHS) and the United States Intelligence Community, ports, depots, stations, and related infrastructure, and stadiums, auditoriums, and large buildings. Additionally, critical infrastructure of primary importance includes nuclear, chemical, biological, and other hazardous material facilities, bridges, tunnels, dams, and power generation/transfer stations, energy facilities including petroleum refining and related industries, and iconic cities and facilities, large buildings, and complex high-density infrastructure.

The possible means of attacking such national interests are far ranging. We know from operational activity around the world that al-Qaida can execute mass-casualty attacks using improvised explosive devices (IEDs) combined with suicide operatives. The capture of operatives overseas this past summer led to the identification of detailed casing reports prepared prior to 9/11. The specific tactics recommended in these reports highlights al-Qaida's ongoing interest and preference for using vehicle-borne improvised explosive devices (VBIEDs) to attack high-profile or symbolic targets.

Al-Qaida has demonstrated operational proficiency in using aircraft as weapons, in particular hijacking operations, and has explored the idea of bringing down aircraft in flight through the use of several different IED configurations. Al-Qaida has also demonstrated a capability to use man-portable air-defense systems (MANPADs) in operations against aircraft overseas, although there are no indications that it plans to use this capability for attacks inside the United States. .

Al-Qaida and its affiliated groups have demonstrated an operational capability to conduct dramatic, mass-casualty attacks against both hard and soft targets inside the United States and abroad. Within this broad operational spectrum, the most severe threats revolve around al-Qaida and its affiliates' long-standing intent to develop, procure, or acquire chemical, biological, radiological, and even nuclear, weapons for mass-casualty attacks. Al-Qaida and affiliated elements currently have the capability to produce small amounts of crude biological toxins and toxic chemical materials, and may have acquired small amounts of radioactive materials. However, we currently assess that al-Qaida has not been able to acquire or develop a functioning nuclear weapon (i.e., one that generates a nuclear yield).

Despite al-Qaida's intent to strike us with Weapons of Mass Effect (WME), we assess that the United States is a "harder target" for the terrorist and for the illegal migrant than it was in the past because of improvements in information sharing and security measures since 9/11. There remain, of course, difficulties in securing the over 95,000 miles of coastline and 7,000 miles of border shared with Canada and Mexico. Indeed, the efforts of DHS have been successful, and the determination of the 180,000 plus Department personnel working around the country and around the world day in and day out is strong and completely dedicated to securing our homeland.

There is much evidence to convince us that interdiction measures have improved; intelligence is working, technology has helped, and far fewer illegal immigrants are now able to enter our ports of entry or cross our borders than in the past. However, we still see persons using fraudulent documentation; many are already on our watch lists, attempting to enter the United States at the borders and at ports of entry. Thus, we assess that the threat of illegal and even covert entry is still present and likely will be for the foreseeable future.

On land, we now have greatly improved systems to keep track of persons who cross the border and we have begun to apply technology to monitor the border where there is no direct border patrol presence. We also believe that fraudulent documentation is far more likely to be discovered than in the past—owing in part to improved technology, better training, more comprehensive data bases, the increased use of biometrics, and better coordination among agencies.

However, entrenched human smuggling networks and corruption in areas beyond our borders can be exploited by terrorist organizations. Recent information from on-

going investigations, detentions, and emerging threat streams strongly suggests that al-Qaida has considered using the Southwest Border to infiltrate the United States. Several al-Qaida leaders believe operatives can pay their way into the country through Mexico and also believe illegal entry is more advantageous than legal entry for operational security reasons. However, there is currently no conclusive evidence that indicates al-Qaida operatives have made successful penetrations into the United States via this method.

In addition to the problems posed by the southwestern border, the long United States-Canada border, often rugged and remote, includes a variety of terrain and waterways, some suitable for illicit border crossings. A host of unofficial border crossings can be utilized when employing the services of alien smugglers, especially those winding through mountain ranges and across the vast western prairie.

In addition to the threats posed at the extensive United States land border, we believe al-Qaida remains focused on targeting civil aviation. Since the creation of the Department in March 2003, DHS has led Federal Government effort to harden and protect the aviation infrastructure. The barriers and checks put in place since 9/11 at airports and the system of baggage and cargo checks for air transported materials have proven very effective in identification and interdiction of unauthorized items and in the identification of persons engaged in air travel. However, al-Qaida operatives have received flight training, and we believe al-Qaida continues to consider new and novel methods for planning and conducting attacks against civil aviation in the United States. Al-Qaida still views the hijacking of commercial passenger aircraft inside the United States as a primary objective.

Other aviation threats include the possible use of ultra-light aircraft or remotely piloted vehicles (RPVs), although we have no specific or credible information suggesting that terrorists have considered these platforms for attacks in the Homeland. Additionally, while al-Qaida has considered conducting an attack against United States interests overseas using helicopters packed with explosives, there is no specific or credible evidence supporting the use of helicopters in aerial attacks within the United States. There have been recent media reports about lasers being visible to pilots in commercial aircraft in the United States. Although no specific or credible information suggests terrorists plan to use high-powered lasers in the United States, groups overseas have expressed interest in using these devices against human sight.

At sea, we see positive changes and advances in the control system similar to those made in land border crossing and aviation. These advancements include improving vessel registration documentation and identification capabilities and better search technologies and procedures. While the complex problem with sea-transported cargo and the checking especially of containers and container vessels remains, significant improvements have been made since 9/11.

Al-Qaida remains the preeminent organization with both intent and capabilities to targets United States maritime assets. A variation of the familiar VBIED, the small, explosiveladen boat usually piloted by a suicide operative, remains al-Qaida's weapon of choice in the maritime environment. In addition to threats posed by terrorist attack, the smuggling of illegal migrants via maritime means continues to be a major concern for homeland security. This threat is expected to grow as organized criminal groups continue to expand their operations throughout the world. The huge profit potential in this trade will ensure that it will remain a lucrative venture for the foreseeable future. The inability of Central American nations to control their borders is also an important factor favoring the smugglers.

Additionally, a small but increasing threat to homeland security is represented by stowaways on merchant vessels and by crewmen jumping ship. Most of these individuals are economic migrants and account for a small fraction of illegal migration. However, their illegal activity highlights persistent border security vulnerabilities that may be exploited by contraband smugglers and terrorist organizations, as well as concerns for merchant vessel and crew safety. When acting alone, stowaways take advantage of poor security in foreign ports to simply walk on board vessels and attempt to stay hidden for the duration of the voyage. However, many stowaway incidents are part of criminally organized attempts to traffic people and require the complicity of merchant ship crewmembers. The threat posed by merchant seamen illegally entering the United States includes deserters who depart the ship legally, but do not return and absconders who illegally depart the ship once in port. The use of these methods by criminals or terrorists to enter the United States is probable.

The bottom line is that the best efforts of the DHS, of the United States Intelligence Community, and of the entire Federal Government are allied against terrorist efforts to stage attacks in the homeland. However, despite these efforts and innumerable advances in information sharing, technology, communication, and orga-

nization, any attack of any kind could occur at any time. While we have not seen a trend by any terrorist group to tie an act of terrorism to a particular date or time, or even place, beyond the obvious goal of striking a locale or transportation mode when a larger number of people might be present, we do not believe we can predict timing unless we are somehow inside the decisionmaking mechanism used by the terrorists.

An attack against the homeland with the most severe ramifications would include the use of a WME, especially nuclear. We also give due respect to the potential for some forms of biological attack to generate high casualty numbers. Beyond that, most attacks would be locally severe and would have larger implications psychologically, culturally, and economically even if their immediate destructive impact was very limited. While we have not seen such methods employed in the homeland to date, we do worry about the possibility of small attacks—the grenade into the outdoor restaurant, the small bomb in the public place, the random shooting on the street—that would ostensibly be carried out to influence U.S. authorities to react strongly in the context of preventing such acts from occurring.

There is a risk of cyber or combined physical-cyber attacks from various malicious actors, though it is difficult to quantify that risk. However, the Intelligence Community believes there is sufficient risk, and while there is no known information that anyone is preparing a significant cyber attack, there appears to be circumstantial evidence that terrorists are using a variety of illegal Internet behaviors to finance their activities.

Given the anecdotal and imprecise nature of information in this regard, it is important to focus on the whole risk picture, including threat, vulnerabilities, and potential consequences. Accordingly, the government is enhancing its interagency coordination through the National Cyber Response Coordination Group (NCRCG) formalized by the Cyber Annex to the National Response Plan to prepare for and respond to national level cyber attacks from any sources and in the Interagency Security Plan (ISP) to reduce our vulnerability to attacks that might cause a major Internet disruption.

Which is the largest of the potential threats to the homeland? Which is the most severe? Which is the most probable? These are questions that cannot realistically be answered beyond the information provided here. We are hesitant to make an attempt to answer these questions beyond stating that, conditionally and circumstantially, any event and any terrorist action is worthy of, and will continue to receive, our full attention and interest.

Chairman Roberts, Senator Rockefeller, and Members of the Committee, this concludes my prepared statement. I would be happy to answer any questions you may have at this time.

Chairman ROBERTS. Well, we thank you, Admiral, for a very comprehensive statement.

I would tell the witnesses that we're having a closed hearing on the threat of nuclear terrorism as of tomorrow. It's my personal belief that if al-Qa'ida could obtain a nuclear weapon or any material and could get it into the U.S., that they would use it. The question is not whether al-Qa'ida would use a nuclear weapon, but can they get one?

Pakistani scientist A.Q. Khan passed secrets and equipment to a host of rogue nations. The Pakistani government has cooperated in our efforts to stop this activity and Mr. Khan is under house arrest in Pakistan.

This is for Director Goss, Admiral Loy. What is your assessment of the current status of the Khan network? Does the fact that he is in custody mean the network is shut down? Are there any other non-state actors that are potential Khans?

And especially for Admiral Loy, what is the Department of Homeland Security's assessment of that threat? You have touched on it in your statement. And more particularly, if you could be very succinct, what steps has your department taken to prevent or to mitigate a terrorist attack utilizing any nuclear weapon?

Director Goss.

Director GOSS. Mr. Chairman, thank you.

Actually, it's timely that you ask that question, because we are further exploring our opportunities to learn about Mr. Khan and what he has done. I am unable to give you the details of that. They would be suitable for a closed hearing. But I can assure you that, virtually as we speak, efforts—active, appropriate direct efforts—are underway on that matter.

We have found, from a variety of sources, following the leads of what we've known already, that we've uncovered many new things. And we have found that in uncovering those things we have not got to the end of the trail. Getting to the end of that trail is extremely important for us.

It is a serious proliferation question. I'm pleased you're having a closed hearing. I'd be very happy to make available those experts in our business who can contribute to your wisdom in a closed session.

Chairman ROBERTS. What about the non-state actors that are potential Khans?

Director GOSS. The potential Khans are a very nervous worry for us, obviously. If there were a way—and that's the big question, how would they go about getting it—would we know and could we stop it?

In some cases, the regimes we have are good enough to understand most of the issue and most of the stocks and where things are supposed to be and how they're supposed to work. But most isn't good enough. You need 100 percent to get to the guarantee that you want.

So, the answer for non-state actors being able to get these kinds of materials, either nuclear, chem or bio, is a reality.

Chairman ROBERTS. Admiral Loy, your assessment of the nuclear terrorism threat? You touched on it in your statement.

Admiral LOY. Briefly, sir, certainly there are three or four that we would categorize as those concerns that keep us awake nights the most. They certainly would include nuclear, chemical, bio and cyber. With respect directly to nuclear, Director Goss has the inside track. I would offer—to offering the most insight to the worldwide nature, with respect to proliferation—our concerns at DHS go more directly to the ability to detect those materials as they might be coming in our direction.

In the President's budget for 2006, there is an initiative that we're referring to as the National Nuclear Detection Office, to be established inside the Department of Homeland Security—not a DHS initiative, but literally a national initiative—wherein the offices and the good capabilities of DoD and DOJ and DOE and all others with equities in the issue can be pooled, such that we can make some kind of an effort that does two things—one, optimizes the deployment of current capability in the areas of detection and, second, fences a significant amount of money—almost a mini-Manhattan Project, if you will—to offer us a chance to break through toward next-generation capability of detection.

Those are the efforts that we have underway, Mr. Chairman. And, again, if there is a closed hearing, we'd be happy to participate.

Chairman ROBERTS. I'm going to change the subject. In the last few years we've had the Joint Inquiry, the 9/11 Commission, this

Committee's review in regards to WMD in Iraq—all of which highlighted the failure to share intelligence information across the intelligence community.

For every intelligence failure, you hear another recommendation for more information sharing. That's the buzzword. For too many times, when we hear about a consensus threat, we find out there's not a consensus. I believe, however, that information sharing is a rather limited idea that falsely implies that the intelligence collectors own the information that they collect.

The Vice Chairman and I also think that information sharing means that the collectors push information to the analysts they believe have a need to know.

I think we need to change our thinking on this issue. It's time to be working toward a more powerful concept. We call it information access. No one agency of the U.S. Government owns intelligence information and any cleared analyst with a need to know should be able to access it.

While sensitive information must still be managed—I know that—cleared analysts should be able to pull that information by searching all intelligence databases without having to wait for any one agency to push the information to them, as we do it today.

What do you think—and I'm addressing, basically, Director Goss here—about this idea of information access, as well as Director Mueller. Do we need to take the classification authority away from the collection agencies and put it in the hands of an authority, i.e., the DNI, who is neither a collector or an analyst, who can more honestly balance the need to know with the need to protect the sources and methods?

Director GOSS. Thank you, Mr. Chairman.

The sources and methods question I am clear on. We do need to protect our sources and methods. The degree that some of our sources and methods are revealed in the media from time to time, through leaks and other matters, does not necessarily mean we shouldn't continue to protect them. Just because it's reported in the paper doesn't mean we're going to confirm it. Sometimes we are able to still get further utility out of sources and methods, even though they have been discussed, because not everybody may read that particular paper.

But it is harmful to us, in our efforts to broaden the product in the community, that not everybody is playing by exactly the same rules. We find that different people treat classifications different ways and have different reactions to it. So I do believe you would be right in focusing some attention on the classification and declassification process. It is clearly an area that needs attention, something we've talked about in the past. And it is still somewhat of a neglected stepchild.

In the area of getting the information to who needs to know, that's exactly on target. The trick is, who needs to know? It was always a question of sharing with who needs to know. The question of who makes that decision of who needs to know has always been the problem.

We find that the audience of who needs to know is, in fact, larger as we bring our community and its many, many elements together

that are being asked to do things—more things—not only overseas, but particularly now at home.

Our domestic agencies—as Admiral Loy has just testified, and as Director Mueller has testified—clearly are doing things in the war on terrorism that require sharing of information. Well, the foreign intelligence program, which is where the intelligence program has always operated, is doing new business with domestic agencies to deal with terrorism in a domestic way, because, as you know, the foreign intelligence program is prohibited from spying on Americans.

So, getting that piece just right has been part of the effort, as we have gone along since 9/11. And I am pleased to report we are doing exceedingly well, in my view, on that. And I would hope that my colleagues would agree. There's still room to go, but I believe we are sharing much better. I certainly agree analysts should be driving collection and not the other way around.

Chairman ROBERTS. I ask for the patience of my colleagues. My time is up, but I would like for Director Mueller to address this, and also Admiral Jacoby.

If you can be short and succinct, sir.

Director MUELLER. I certainly agree with the premise that those responsible for acting should have access to the information in whatever database it resides, in whatever agency.

I think TTIC, the Terrorist Threat Integration Center, and the National Counterterrorism Center, when it comes to terrorism information, has taken us well along that way to give us access to the information, regardless of in which database it resides. Co-location, as we've co-located out in Tyson, has helped immeasurably to break down some of those barriers.

So, I agree with the premise. I also agree with, I think, the second premise. And that is the importance of the analysts having access to at least information relating to the motivations of underlying sources, the access that the underlying source may have to the information. Having more clarity as to what moves the person to provide the information, to whether it be the FBI, CIA or elsewhere. And that, I think, is something we have to work on.

Last, in terms of moving the authority from the agency to the DNI, I do think the agency, at the outset, needs the authority to protect its sources and methods, but it should be reviewed by the DNI. I don't think that moving it up to the DNI would work all that well. But I do believe that the DNI ought to review how we classify, how we describe our sources and methods.

Chairman ROBERTS. Admiral Jacoby.

STATEMENT OF VICE ADMIRAL LOWELL JACOBY, USN, DIRECTOR, DEFENSE INTELLIGENCE AGENCY

Admiral JACOBY. Sir, your ownership of information statement is just right on the mark, sir. I think that's a desperately important area for this Committee and for our community to continue to work hard on.

Part of it that comes along with the need to know is, the way we do business today, the collector decides who needs to know in many cases. We need to swap that and have the analysts who are

charged with discovering information and generating knowledge be the driver in the process.

The other part that's desperately important to this is putting in place the Smart Network that is talked about so concisely in the 9/11 Commission report, because applying modern commercial information management kinds of tools will help us to separate the content from neglected information while still protecting the sourcing of the information. That's a desperately important part of this whole discussion and needs to be pursued very aggressively.

[The prepared statement of Admiral Jacoby follows:]

PREPARED STATEMENT OF VICE ADMIRAL LOWELL E. JACOBY,
U.S. NAVY DIRECTOR, DEFENSE INTELLIGENCE AGENCY

Good morning Mr. Chairman, Mr. Vice Chairman and Members of the Committee. It is my honor and privilege to represent Defense Intelligence and present what we know and believe to be the principal threats and issues in today's world. The dedicated men and women of Defense Intelligence work around the clock and around the world to protect our country. Many of these active duty, reserve and civilian intelligence professionals are working in remote and dangerous conditions. Our mission is simple, but rarely easy. It is to discover information and create knowledge to provide warning, identify opportunities and deliver overwhelming advantage to our warfighters, defense planners and national security policymakers.

This is the third time I report to you that Defense Intelligence is engaged in a war on a global scale. Most of the forces and issues involved in this war were addressed in my testimony last year. Several increased in severity or changed in composition. Few, unfortunately, decreased.

The traditional Defense Intelligence focus on military capabilities is insufficient to identify and gauge the breadth of these threats. We are working hard to access "all" information to better understand and counter these threats. Defense Intelligence is engaged with foreign and domestic counterparts to better integrate our capabilities. We remained focused on information sharing and creating the "smart networks" described in the 9/11 Commission report. I am anxious to work with the new Director of National Intelligence, my fellow intelligence agency heads and others to forge a more cohesive and comprehensive Intelligence Community.

GLOBAL WAR ON TERRORISM

We continue to face a variety of threats from terrorist organizations.

Al-Qaida and Sunni Extremist Groups. The primary threat for the foreseeable future is a network of Islamic extremists hostile to the United States and our interests. The network is transnational and has a broad range of capabilities, to include mass-casualty attacks. The most dangerous and immediate threat is Sunni Islamic terrorists that form the "al-Qaida associated movement."

Usama bin Ladin and his senior leadership no longer exercise centralized control and direction. We now face an "al-Qaida associated movement" of like-minded groups who interact, share resources and work to achieve shared goals. Some of the groups comprising this movement include Jemaah Islamiyya, responsible for the 9 September bombing of the Australian Embassy in Jakarta and Hezb-e-Islami-Gulbuddin. Some of the groups in the movement provide safe haven and logistical support to al-Qaida members, others operate directly with al-Qaida and still others fight with al-Qaida in the Afghanistan/Pakistan region.

Remnants of the senior leadership still present a threat. As is clear in their public statements, Bin Ladin and al-Zawahiri remain focused on their strategic objectives, including another major casualty-producing attack against the Homeland.

CBRN Terrorism. We judge terrorist groups, particularly al-Qaida, remain interested in Chemical, Biological, Radiological and Nuclear (CBRN) weapons. Al Qaida's stated intention to conduct an attack exceeding the destruction of 9/11 raises the possibility that planned attacks may involve unconventional weapons. There is little doubt it has contemplated using radiological or nuclear material. The question is whether al-Qaida has the capability. Because they are easier to employ, we believe terrorists are more likely to use biological agents such as ricin or botulinum toxin or toxic industrial chemicals to cause casualties and attack the psyche of the targeted populations.

Pressures in the Islamic World. Various factors coalesce to sustain, and even magnify the terrorist threat.

Islam is the world's second largest religion with over 1 billion adherents, representing 22 percent of the world's population. Due to high birth rates, it is also the world's fastest growing religion. Only twenty percent of Muslims are ethnic Arabs. The top four nations in terms of Muslim population, Indonesia, Pakistan, Bangladesh and India, are non-Arab. While the vast majority of Muslims do not advocate violence, there are deeply felt sentiments that cross Muslims sects and ethnic and racial groups.

Our policies in the Middle East fuel Islamic resentment. Multiple polls show favorable ratings for the United States in the Muslim world at all-time lows. A large majority of Jordanians oppose the War on Terrorism, and believe Iraqis will be "worse off' in the long term. In Pakistan, a majority of the population holds a "favorable" view of Usama bin Ladin. Across the Middle East, surveys report suspicion over U.S. motivation for the War on Terrorism. Overwhelming majorities in Morocco, Jordan, and Saudi Arabia believe the U.S. has a negative policy toward the Arab world.

Usama bin Ladin has relied on Muslim resentment toward U.S. policies in his call for a defensive jihad to oppose an American assault on the Islamic faith and culture. He contends that all faithful Muslims are obliged to fight, or support the jihad financially if not physically capable of fighting. Another goal is the overthrow of "apostate" Muslim governments, defined as governments which do not promote Islamic values or support or are friendly to the U.S. and other Western countries. The goals also call for withdrawal of U.S. and other Coalition forces from Muslim countries, the destruction of Israel and restoration of a Palestinian State and recreation of the caliphate, a State based on Islamic fundamental tenets.

Underlying the rise of extremism are political and socio-economic conditions that leave many, mostly young male adults, alienated. There is a demographic explosion or youth bubble in many Muslim countries. The portion of the population under age 15 is 40 percent in Iraq, 49 percent in the Gaza Strip and 38 percent in Saudi Arabia. Unemployment rates in these countries are as high as 30 percent in Saudi Arabia and about 50 percent in the Gaza Strip.

Educational systems in many nations contribute to the appeal of Islamic extremism. Some schools, particularly the private "madrasas," actively promote Islamic extremism. School textbooks in several Middle East states reflect a narrow interpretation of the Koran and contain anti-Western and anti-Israeli views. Many schools concentrate on Islamic studies focused on? memorization and recitation of the Koran and fail to prepare students for jobs in the global economy.

Groups like al-Qaida capitalize on the economic and political disenfranchisement to attract new recruits. Even historically local conflicts involving Muslim minorities or fundamentalist groups such as those in Indonesia, the Philippines and Thailand are generating new support for al-Qaida and present new al-Qaida-like threats.

Saudi-Arabia. Al Saud rule is under significant pressure. In 2004, 15 significant attacks occurred against the regime, U.S. and other Western targets in the Kingdom, an increase from 7 in 2003. Attacks in 2004 included the 6 December 2004 attack on the U.S. Consulate in Jeddah.

Attacks since May 2003 against housing compounds, an Interior Ministry facility, a petroleum facility and individual assassinations caused Riyadh to attempt to aggressively counter the threat. We expect continued assassinations, infrastructure attacks and operations directed at Westerners in the Kingdom to discredit the regime and discourage individuals and businesses, especially those affiliated with the Saudi military, from remaining in the Kingdom.

Last year Saudi security forces killed or captured many of their 26 most wanted militant extremists and discovered numerous arms caches. However, we believe there may be hundreds, if not thousands of extremists and extremist sympathizers in the Kingdom.

Pakistan. President Musharraf continues to be a key ally in the War on Terrorism and provides critical support against Al-Qaida and Taliban operating in Pakistan. The economy has displayed strong growth over the past 2 years. Indigenous and international terrorist groups have pledged to assassinate Musharraf and other senior Pakistan government officials and remain a significant threat. Unless Musharraf is assassinated, Pakistan will remain stable through the year; however, further political and economic reform is needed to continue positive trends beyond that time.

Pakistan significantly increased its military operations and pacification efforts in tribal areas along the Afghanistan border in 2004. These operations affected al-Qaida, Taliban, and other threat groups by disrupting safe-havens and, in some cases, forcing them back into Afghanistan where they are vulnerable to Coalition operations. Pakistan also secured agreements with several tribes by successfully balancing military action with negotiations and rewards to encourage cooperation

and limit domestic backlash. Pakistan must maintain and expand these operations in order to permanently disrupt insurgent and terrorist activity.

We believe international and indigenous terrorist groups continue to pose a high threat to senior Pakistani government officials, military officers and U.S. interests. The Prime Minister and a corps commander have been the targets of assassination attempts since last summer. President Musharraf remains at high risk of assassination, although no known attempts on his life have occurred since December 2003. Investigations into the two December 2003 attempts revealed complicity among junior officers and enlisted personnel in the Pakistani Army and Air Force.

Our assessment remains unchanged from last year. If Musharraf were assassinated or otherwise replaced, Pakistan's new leader would be less pro-US. We are concerned that extremist Islamic politicians would gain greater influence.

CONFLICT IN IRAQ

The insurgency in Iraq has grown in size and complexity over the past year. Attacks numbered approximately 25 per day 1 year ago. Today, they average in the 60s. Insurgents have demonstrated their ability to increase attacks around key events such as the Iraqi Interim Government (IIG) transfer of power, Ramadan and the recent election. Attacks on Iraq's election day reached approximately 300, double the previous 1 day high of approximately 150 reached during last year's Ramadan.

The pattern of attacks remains the same as last year. Approximately 80 percent of all attacks occur in Sunni-dominated central Iraq. The Kurdish north and Shia south remain relatively calm. Coalition Forces continue to be the primary targets. Iraqi Security Forces and Iraqi Interim Government (IIG) officials are attacked to intimidate the Iraqi people and undermine control and legitimacy. Attacks against foreign nationals are intended to intimidate non-government organizations and contractors and inhibit reconstruction and economic recovery. Attacks against the country's infrastructure, especially electricity and the oil industry, are intended to stall economic recovery, increase popular discontent and further undermine support for the IIG and Coalition.

Recent polls show confidence in the Iraqi Interim Government remains high in Shia and Kurdish communities and low in Sunni areas. Large majorities across all groups opposed attacks on Iraqi Security Forces and Iraqi and foreign civilians. Majorities of all groups placed great importance in the election. Sunni concern over election security likely explains the relatively poor showing by the Sunni electorate in comparison with the Shia and Kurdish groups. Confidence in Coalition Forces is low. Most Iraqis see them as occupiers and a major cause of the insurgency.

We believe Sunni Arabs, dominated by Ba'athist and Former Regime Elements (FRE), comprise the core of the insurgency. Ba'athist/FRE and Sunni Arab networks are likely collaborating, providing funds and guidance across family, tribal, religious and peer group lines. Some coordination between Sunni and Shia groups is also likely.

Militant Shia elements, including those associated with Muqtada al Sadr, have periodically fought the Coalition. Following the latest round of fighting last August and September, we judge Sadr's forces are re-arming, re-organizing and training. Sadr is keeping his options open to either participate in the political process or employ his forces. Shia militants will remain a significant threat to the political process and fractures within the Shia community are a concern.

Jihadists, such as al-Qaida operative Abu Musab al Zarqawi, are responsible for many high-profile attacks. While Jihadist activity accounts for only a fraction of the overall violence, the strategic and symbolic nature of their attacks, combined with effective Information Operations, has a disproportionate impact.

Foreign fighters are a small component of the insurgency and comprise a very small percentage of all detainees. Syrian, Saudi, Egyptian, Jordanian and Iranian nationals make up the majority of foreign fighters. Fighters, arms and other supplies continue to enter Iraq from virtually all of its neighbors despite increased border security.

Insurgent groups will continue to use violence to attempt to protect Sunni Arab interests and regain dominance. Subversion and infiltration of emerging government institutions, security and intelligence services will be a major problem for the new government. Jihadists will continue to attack in Iraq in pursuit of their long-term goals. Challenges to reconstruction, economic development and employment will continue. Keys to success remain improving security with an Iraqi lead, rebuilding the civil infrastructure and economy and creating a political process that all major ethnic and sectarian groups see as legitimate.

CONFLICT IN AFGHANISTAN

The people of Afghanistan achieved a major milestone by electing Hamid Karzai president in October 2004 election. Approximately 70 percent or just over 8 million registered Afghans disregarded scattered attacks by the Taliban and al-Qaida and voted. Karzai garnered 55 percent of the vote in a field of 18 candidates. The election dealt a blow to insurgents and provides new momentum for reform, such as the demobilization of private militias and increased government accountability.

President Karzai has since assembled a cabinet of reform minded and competent ministers who are ethnically and politically diverse. Most significantly, he removed Afghanistan's most powerful warlord, Marshal Fahim Khan, as Defense Minister.

Despite the overwhelming voter turn-out, the election's results highlighted ethnic divisions. Karzai received a majority of the Pashtun vote, but failed to do so within any of the other ethnic groups. Continued ethnic divisions remain a challenge to political stability. National Assembly elections, scheduled for later this year, will provide the opportunity for non-Pashtuns to increase their participation in the government.

The security situation improved over the past year. Insurgent attacks precipitously dropped after Afghanistan's presidential election. The primary targets remain Coalition Forces and facilities in the southern and eastern provinces. Voter registration teams and polling sites were attacked in these areas, reflecting the Taliban's concern over legitimate elections. Similar attacks in the same geographic areas are expected for elections later this year, but are unlikely to have a significant impact.

We believe many Taliban leaders and fighters were demoralized by their inability to derail the election and have seen their base of support among Pashtun tribes decrease. Loss of support, plus continued Coalition and Pakistani military operations, have prompted some to express an interest in abandoning the insurgency and pursuing political alternatives. Nevertheless some factions will likely remain committed to the insurgency and seek funding to continue operations.

WEAPONS OF MASS DESTRUCTION AND MISSILE PROLIFERATION

Nuclear Weapons. Immediately behind terrorism, nuclear proliferation remains the most significant threats to our Nation and international stability. We anticipate increases in the nuclear weapons inventories of a variety of countries to include China, India, Pakistan and North Korea.

Iran is likely continuing nuclear weapon-related endeavors in an effort to become the dominant regional power and deter what it perceives as the potential for U.S. or Israeli attacks. We judge Iran is devoting significant resources to its weapons of mass destruction and ballistic missile programs. Unless constrained by a nuclear non-proliferation agreement, Tehran probably will have the ability to produce nuclear weapons early in the next decade.

With declining or stagnant conventional military capabilities, we believe North Korea considers nuclear weapons critical to deterring the U.S. and ROK. After expelling IAEA personnel in 2002, North Korea reactivated facilities at Yongbyon and claims it extracted and weaponized plutonium from the 8,000 spent fuel rods. Only last week, Pyongyang publicly claimed it had manufactured nuclear weapons. Kim Chong-il may eventually agree to negotiate away parts of his nuclear weapon stockpile and program and agree to some type of inspection regime, but we judge Kim is not likely to surrender all of his nuclear weapon capabilities. We do not know under what conditions North Korea would sell nuclear weapons or technology.

India and Pakistan continue to expand and modernize their nuclear weapon stockpiles. We remain concerned over the potential for extremists to gain control of Pakistani nuclear weapons. Both nations may develop boosted nuclear weapons, with increased yield.

Chemical and Biological Weapons. Chemical and biological weapons pose a significant threat to our deployed forces, international interests and homeland. Numerous states have chemical and biological warfare programs. Some have produced and weaponized agents. While we have no intelligence suggesting these states are planning to transfer weapons to terrorist groups, we remain concerned and alert to the possibility.

We anticipate the threat posed by biological and chemical agents will become more diverse and sophisticated over the next 10 years. Major advances in the biological sciences and information technology will enable BW agent—both anti-human and anti-agricultural—development. The proliferation of dual use technology compounds the problem. Many states will remain focused on "traditional" BW or CW agent programs. Others are likely to develop non-traditional chemical agents or use advanced biotechnology to create agents that are more difficult to detect, easier to produce, and resistant to medical countermeasures.

Ballistic Missiles. Moscow likely views its strategic forces, especially its nuclear armed missiles, as a symbol of great power status and a key deterrent. Nevertheless, Russia's ballistic missile force will continue to decline in numbers. Russia is fielding the silo-variant of the SS–27 Intercontinental Ballistic Missile (ICBM) and is developing a road-mobile variant and may be developing another new ICBM and new Submarine Launched Ballistic Missile (SLBM). It recently developed and is marketing anew Short Range Ballistic Missile (SRBM). Russia also is trying to preserve and extend the lives of Soviet-era missile systems.

China is modernizing and expanding its ballistic missile forces to improve their survivability and war-fighting capabilities, enhance their coercion and deterrence value and overcome ballistic missile defense systems. This effort is commensurate with its growing power and more assertive policies, especially with respect to Taiwan. It continues to develop three new solid-propellant strategic missile systems—the DF–31 and DF–31A road-mobile ICBMs and the JL–2 SLBM. By 2015, the number of warheads capable of targeting the continental United States will increase several fold.

China also is developing new SRBMs, Medium Range Ballistic Missile (MRBMs), and Intermediate Range Ballistic Missile (ICBMs). They are a key component of Beijing's military modernization program. Many of these systems will be fielded in military regions nearTaiwan. In 2004, it added numerous SRBMs to those already existing in brigades near Taiwan. In addition to key Taiwanese military and civilian facilities, Chinese missiles will be capable of targeting U.S. and allied military installations in the region to either deter outside intervention in a Taiwan crisis or attack those installations if deterrent efforts fail.

We judge Iran will have the technical capability to develop an ICBM by 2015. It is not clear whether Iran has decided to field such a missile. Iran continues to field 1300-km range Shahab III MRBMs capable of reaching Tel Aviv. Iranian officials have publicly claimed they are developing a new 2000-km-range variant of the Shahab III. Iranian engineers are also likely working to improve the accuracy of the country's SRBMs.

North Korea continues to invest in ballistic missiles to defend itself against attack, achieve diplomatic advantage and provide hard currency through foreign sales. Its Taepo Dong 2 intercontinental ballistic missile may be ready for testing. This missile could deliver a nuclear warhead to parts of the United States in a two stage variant and target all of North America with a three stage variant. North Korean also is developing new SRBM and IRBM missiles that will put U.S. and allied forces in the region at further risk.

Pakistan and India continue to develop new ballistic missiles, reflecting tension between those two countries and New Delhi's desire to become a greater regional power. Pakistan flighttested its new solid-propellant MRBM for the first time in 2004. The Indian military is preparing to field several new or updated SRBMs and an MRBM. India is developing a new IRBM, the Agni III.

Syria continues to improve its missile capabilities, which it likely considers essential compensation for conventional military weakness. Syria is fielding updated SRBMs to replace older and shorter-range variants.

Several nations are developing technologies to penetrate ballistic missile defenses.

Cruise Missiles. Land-Attack Cruise Missiles (LACMs) and Lethal Unmanned Aerodynamic Vehicles (LUAVs) are expected to pose an increased threat to deployed U.S. and allied forces in various regions. These capabilities are already emerging in Asia.

The numbers and capabilities of cruise missiles will increase, fueled by maturation of land-attack and Anti-Ship Cruise Missile (ASCM) programs in Europe, Russia, and China, sales of complete systems, and the spread of advanced dual-use technologies and materials. Countering today's ASCMs is a challenging problem and the difficulty in countering these systems will increase with the introduction of more advanced guidance and propulsion technologies. Several ASCMs will have a secondary land-attack role.

China continues developing LACMs. We judge by 2015, it will have hundreds of highly accurate air- and ground-launched LACMs. China is developing and purchasing ASCMs capable of being launched from aircraft, surface ships, submarines, and land that will be more capable of penetrating shipboard defenses. These systems will present significant challenges in the event of a U.S. naval force response to a Taiwan crisis.

In the next 10 years, we expect other countries to join Russia, China, and France as major exporters of cruise missiles. Iran and Pakistan, for instance, are expected to develop or import LACMs. India, in partnership with Russia, will begin production of the PJ–10, an advanced anti-ship and land attack cruise missile, this year.

Major Exporters. Russia, China and North Korea continue to sell WMD and missile technologies for revenue and diplomatic influence. The Russian government, or entities within Russia, continues to support missile programs and civil nuclear projects in China, Iran, India and Syria. Some of the civil nuclear projects can have weapons applications. Chinese entities continue to supply key technologies to countries with WMD and missile programs, especially Pakistan, North Korea and Iran, although China appears to be living up to its 1997 pledge to limit nuclear cooperation with Iran. North Korea remains the leading supplier of missiles and technologies. In recent years, some of the states developing WMD or ballistic missile capabilities have become producers and potential suppliers. Iran has supplied liquid-propellant missile technology to Syria, and has marketed its new solid-propellant SRBM.

We also are watching non-government entities and individual entrepreneurs. The revelations regarding the A.Q. Khan nuclear proliferation network show how a complex international network of suppliers with the requisite expertise and access to the needed technology, middlemen and front companies can successfully circumvent international controls and support multiple nuclear weapons programs.

NATIONS OF INTEREST

Iran. Iran is important to the U.S. because of its size, location, energy resources, military strength and antipathy to U.S. interests. It will continue support for terrorism, aid insurgents in Iraq and work to remove the U.S. from the Middle East. It will also continue its weapons of mass destruction and ballistic missile programs. Iran's drive to acquire nuclear weapons is a key test of international resolve and the nuclear non-proliferation treaty.

Iran's long-term goal is to see the U.S. leave Iraq and the region. Another Iranian goal is a weakened, decentralized and Shia-dominated Iraq that is incapable of posing a threat to Iran. These goals and policies most likely are endorsed by senior regime figures.

Tehran has the only military in the region that can threaten its neighbors and Gulf stability. Its expanding ballistic missile inventory presents a potential threat to states in the region. As new longer range MRBMs are fielded Iran will have missiles with ranges to reach many of our European allies. Although Iran maintains a sizable conventional force, it has made limited progress in modernizing its conventional capabilities. Air and air defense forces rely on out-of-date US, Russian and Chinese equipment. Ground forces suffer from personnel and equipment shortages. Ground forces equipment is also poorly maintained.

We judge Iran can briefly close the Strait of Hormuz, relying on a layered strategy using predominately naval, air, and some ground forces. Last year it purchased North Korean torpedo and missile-armed fast attack craft and midget submarines, making marginal improvements to this capability.

The Iranian government is stable, exercising control through its security services. Few anti-government demonstrations occurred in 2004. President Khatami will leave office in June 2005 and his successor will almost certainly be more conservative. The political reform movement has lost its momentum. Pro-reform media outlets are being closed and leading reformists arrested.

Syria. Longstanding Syrian policies of supporting terrorism, relying on WMD for strategic deterrence, and occupying Lebanon remain largely unchanged. Damascus is providing intelligence on al-Qaida for the War on Terrorism. Its response to U.S. concerns on Iraq has been mixed. Men, material and money continue to cross the Syrian-Iraqi border likely with help from corrupt or sympathetic local officials.

Damascus likely sees opportunities and risks with an unstable Iraq. Syria sees the problems we face in Iraq as beneficial because our commitments in Iraq reduce the prospects for action against Syria. However, Damascus is probably concerned about potential spill-over of Iraqi problems, especially Sunni extremism, into Syria. We see little evidence of active regime support for the insurgency, but Syria offers safe-haven to Iraqi Baathists, some of whom have ties to insurgents.

Syria continues to support Lebanese Hizballah and several rejectionist Palestinian groups, which Damascus argues are legitimate resistance groups.

Syria is making minor improvements to its conventional forces. It is buying modern antitank guided missiles and overhauling some aircraft, but cannot afford major weapon systems acquisitions.

President Bashar al-Asad is Syria's primary decisionmaker. Since becoming President in 2000 upon the death of his father, Asad has gradually replaced long-serving officials. Potential domestic opposition to his rule—such as the Muslim Brotherhood—is weak and disorganized. We judge the Syrian regime is currently stable, but internal or external crises could rapidly threaten it.

China. We do not expect Communist Party Secretary and President Hu Jintao's succession to chairman of the Central Military Command (CMC) to significantly alter Beijing's strategic priorities or its approach to military modernization. The commanders of the People's Liberation Army (PLA) Air Force, Navy, and Second Artillery (Strategic Rocket Forces) joined the CMC in September, demonstrating an institutional change to make China's military more "joint." The CMC traditionally was dominated by generals from PLA ground forces.

China remains keenly interested in Coalition military operations in Afghanistan and Iraq and is using lessons from those operations to guide PLA modernization and strategy. We believe several years will be needed before these lessons are incorporated into the armed forces. We judge Beijing remains concerned over U.S. presence in Iraq, Afghanistan and Central Asia. Beijing may also think it has an opportunity to improve diplomatic and economic relations, to include access to energy resources, with other countries distrustful or resentful of U.S. policy.

China continues to develop or import modern weapons. Their acquisition priorities appear unchanged from my testimony last year. Priorities include submarines, surface combatants, air defense, ballistic and anti-ship cruise missiles and modern fighters. China recently launched a new conventional submarine and acquired its first squadron of modern Su30/FLANKER aircraft for the naval air forces from Russia. The PLA must overcome significant integration challenges to turn these new, advanced and disparate weapon systems into improved capabilities. Beijing also faces technical and operational difficulties in numerous areas. The PLA continues with its plan to cut approximately 200,000 soldiers from the Army to free resources for further modernization, an initiative it began in 2004.

Beijing was likely heartened by President Chen Shui-bian coalition's failure to achieve a majority in the recent Legislative Yuan elections. We believe China has adopted a more activist strategy to deter Taiwan moves toward independence that will stress diplomatic and economic instruments over military pressure. We believe China's leaders prefer to avoid military coercion, at least through the 2008 Olympics, but would initiate military action if it felt that course of action was necessary to prevent Taiwan independence.

Beijing remains committed to improving its forces across from Taiwan. In 2004, it added numerous SRBMs to those already existing in brigades near Taiwan. It is improving its air, naval and ground capabilities necessary to coerce Taiwan unification with the mainland and deter U.S. intervention. Last fall, for instance, a Chinese nuclear submarine conducted a deployment that took it far into the western Pacific Ocean, including an incursion into Japanese waters.

North Korea. After more than a decade of declining or stagnant economic growth, Pyongyang's military capability has significantly degraded. The North's declining capabilities are even more pronounced when viewed in light of the significant improvements over the same period of the ROK military and the US-ROK Combined Forces Command. Nevertheless, the North maintains a large conventional force of over one million soldiers, the majority of which we believe are deployed south of Pyongyang.

North Korea continues to prioritize the military at the expense of its economy. We judge this "Military First Policy" has several purposes. It serves to deter US-ROK aggression. Nationwide conscription is a critical tool for the regime to socialize its citizens to maintain the Kim family in power. The large military allows Pyongyang to use threats and bravado in order to limit US-ROK policy options. Suggestions of sanctions, or military pressure by the U.S. or ROK are countered by the North with threats that such actions are "an act of war" or that it could "turn Seoul into a sea of fire." Inertia, leadership perceptions that military power equals national power and the inability for the regime to change without threatening its leadership also explains the continuing large military commitment.

The North Korean People's Army remains capable of attacking South Korea with artillery and missile forces with limited warning. Such a provocative act, absent an immediate threat, is highly unlikely, counter to Pyongyang's political and economic objectives and would prompt a South Korean-CFC response it could not effectively oppose.

Intemally, the regime in Pyongyang appears stable. Tight control over the population is maintained by a uniquely thorough indoctrination, pervasive security services and Party organizations, and a loyal military.

Russia. Despite an improving economy, Russia continues to face endemic challenges related to its post-Soviet military decline. Seeking to portray itself as a great power, Moscow has made some improvements to its armed forces, but has not addressed difficult domestic problems that will limit the scale and scope of military recovery.

Russian conventional forces have improved from their mid–1990s low point. Moscow nonetheless faces challenges if it is to move beyond these limited improvements.

Significant procurement has been postponed until after 2010 and the Kremlin is not spending enough to modernize Russia's defense industrial base. Russia also faces increasingly negative demographic trends and military quality of life issues that will create military manning problems.

Moscow has been able to boost its defense spending in line with its recovering economy. Russia's Gross National Product averaged 6.7 percent growth over the past 5 years, predominately from increased energy prices and consumer demand. Defense should continue to receive modest real increases in funding, unless Russia suffers an economic setback.

Russia continues vigorous efforts to increase its sales of weapons and military technology. Russia's annual arms exports average several billion dollars. China and India account for the majority of Russia's sales, with both countries buying advanced conventional weapons, production licenses, weapon components and technical assistance to enhance their R&D programs. Efforts to increase its customer base last year resulted in increased sales to Southeast Asia. Russian sales are expected to remain several billion dollars annually for the next few years.

Russia's struggle with the Chechen insurgency continues with no end in sight. Chechen terrorists seized a North Ossetian primary school where over 330 people were killed and two Russian civilian airliners were bombed in flight last summer. Rebels continue targeting Russians in Chechnya and Chechen officials cooperating with Moscow. While Moscow is employing more pro-Russian Chechen security forces against the insurgents, the war taxes Russian ground forces. Although the Chechnya situation remains a minor issue to the average Russian, concerns over spreading violence prompted new government security initiatives and offered cover for imposition of authoritarian political measures.

Russian leaders continue to characterize Operation IRAQI FREEDOM and NATO enlargement as mistakes. They express concerns that U.S. operations in Iraq are creating instability and facilitating terrorism. Russian leaders want others to view the Chechen conflict as a struggle with international terrorism and accuse those who maintain contact with exiled Chechen leaders or criticize Moscow's policies toward Chechnya as pursuing a double standard. Russian officials are wary of potential U.S. and NATO force deployments near Russia or in the former Soviet states. Concern that Ukraine under a President Yushchenko would draw closer to NATO and the EU was a factor motivating Russia's involvement in Ukraine's presidential election.

CLOSING THOUGHTS

This year my testimony focuses on what I believe to be the most immediate threats to our Nation and challenges to our interests. The threat from terrorism has not abated. While our strategic intelligence on terrorist groups is generally good, information on specific plots is vague, dated or sporadic. We can and must do better. Improved collection and analysis capabilities can make a significant difference. We are increasing our ability to provide that timely, relevant intelligence.

The Intelligence Community as a whole needs to improve its collection and focus more analytic resources on pressures in the Islamic world so that we can better understand the drivers for extremism. We also need greater collection and more analytic resources devoted to certain key Islamic countries. We have taken steps to improve our collection and analysis, hiring more individuals with Arabic and Farsi language skills. Nevertheless, more needs to be done across the Intelligence Community, particularly in the area of meaningful, penetrating collection and making the content of that collection available to all who need it.

Proliferation of Weapons of Mass Destruction and Missiles is my second priority. Collection must be improved. Additionally, improving our analytic techniques, adoption of true "all-source" analysis approaches and greater information sharing will help us avoid problems similar to those in our pre-war analysis of Iraq's WMD program.

We also must not let our focus on numerous nations of interest wane. Traditional military intelligence disciplines must remain robust if we are to provide our national security policymakers, defense planners and warfighters the information they need to successfully execute their missions. We need improved collection so that we are stealing our true secrets. There are significant gaps in our understanding of several nations' leaderships' plans and intentions. Additionally, more collection and analysis is needed to provide adequate warning of attack and a more complete understanding of the military capability, doctrine and war plans of numerous countries. We are working to better target collection against these hard targets.

As I mentioned, the threats and challenges I briefed today are the most significant and immediate. They are certainly not the only ones. In previous years, I have

spoken about the security situation in Africa, Latin America and South and Southeast Asia. I also addressed my concerns on information operations, international crime, problems associated with globalization, uneven economic development and ungoverned states. Those issues remain significant concerns and the focus of collection and analytic resources for defense intelligence. We will be requesting additional funding and billets to ensure we retain coverage and reporting on global coverage. We are reallocating our analytic capabilities, implementing the "Master, Measure and Monitor" concept in the Defense Intelligence Analysis Program to better address many of these threats and disturbing trends.

Let me conclude by making two points. First, DIA is focused on transforming its capabilities in all of its mission areas to operate in a true "all-source" environment. We are committed to incorporating all relevant information into our analyses, integrating analysts with collectors and precisely targeting our analytic and collection capabilities against complex threats and tough issues. More opportunity for "discovery," greater penetration of hard targets and higher confidence in our judgments are our goals. Second, we are aggressively reengineering our information management approach and architecture. We are focused on harvesting non-traditional sources of data and positioning ourselves to exploit information from new and future sources. We are convinced commercial sector "content management practices" and data standards hold the key to upgrading our information management capability and providing the "smart network" we need. Much more work is required in the area if we are to realize our potential and fundamentally improve our capabilities. These efforts follow the Director of Central Intelligence and the Secretary of Defense guidance and reflect the letter and spirit of the intelligence reform act. Thank you. I look forward to your questions.

Chairman ROBERTS. Admiral Loy and Ms. Rodley, I apologize for not asking for your response in the interest of time. But I would just say, from the INR aspect, I know the Vice Chairman and I and Members of this Committee want to thank you. You're one agency that got it right in regards to the WMD situation. And both of you have a very strong interest in this.

Senator Rockefeller and I apologize to my colleagues.

Vice Chairman ROCKEFELLER. Thank you, Mr. Chairman.

I just second what the Chairman has indicated. I refer to sharing and access. If you share, it's the decision to give. It's a decision on the part of the holder. If it's access, then it is the right of the receiver. So, sharing out/getting in. And I think that will be worked out over the years.

Director Goss, the National Intelligence Council recently issued its annual report to Congress on the safety and the security of Russian nuclear facilities and military forces. The report is both classified and unclassified. One excerpt from the unclassified version is as follows:

"Russian officials have reported that terrorists have targeted Russian nuclear weapons storage sites. Security was tightened in 2001, after Russian authorities twice thwarted terrorist efforts to reconnoiter nuclear weapon storage sites.

"We find it"—this is a continuation of the report, unclassified—"we find it highly unlikely that Russian authorities would have been able to recover all the material reportedly stolen. We assess that undetected smuggling has occurred and we are concerned about the total amount of material that could be diverted or stolen in the last 13 years."

Now, I'd ask you, sir, is the material missing from Russian nuclear facilities sufficient to construct a nuclear weapon?

Director GOSS. Senator, the way I would prefer to answer that question, is there is sufficient material unaccounted for, so that it would be possible for those with know-how to construct a nuclear weapon. I hope that's sufficiently clear.

Vice Chairman ROCKEFELLER. We'll wait for a closed session.

On the same subject, the National Intelligence Council assessment, can you assure the American people—and I think this is a yes-or-no type thing—can you assure the American people that the material missing from Russian nuclear sites has not found its way into terrorist hands?

Director GOSS. No. I can't make that assurance. I can't account for some of the material, so I can't make the assurance about its whereabouts.

Vice Chairman ROCKEFELLER. Appreciate it, sir.

Africa. Since the 1980s, a million people have died of starvation, enormous dislocation, poverty, hopelessness, despair, instability, a fertile breeding ground for terrorism, both east and west, a large Islamic population. Instability in the African continent has allowed us to intervene episodically back and forth.

But the whole prospect of the concept that this is the next great threat, and that being something called a failed continent, General James Jones made that point to the Chairman and me three times in a presentation in London, when he was stationed there. He said, this is the continent that you in the intelligence world need to be looking at—a failed continent, because we are consumed by challenges in Iraq, necessarily, Afghanistan and other world hotspots.

Again, Director Goss, are we facing the possibility, do you think, of the collapse of civil society throughout much of Africa? Shouldn't we be addressing the problems in these countries now, rather than at a future date when our options will be more likely to be military?

Director GOSS. Senator, thank you.

As you know, I've made the statement many times that I don't want to get into the Department of State's policy areas, and the question you've asked me gets into actually a much bigger question than just the intelligence community. But it's a great question. And you are right on the mark, that this is an over-neglected area that is under-resourced for American interests, from my perspective.

I can tell you that I have read Kaplan's piece about the resurgence of anarchy and I've read Friedman's pieces on this. We have have seen all kinds of very nasty people, Foday Sankoh, people like that in the past, who have taken advantage of exploitation of the processes there.

We find that we are going backwards in some areas where we should be going forwards. You heard me mention in my remarks a whole series of bands, of arcs, as it were, of different kinds of problems in Africa. I think it is a rich seabed for people who have a mission on their mind to go and try and recruit people. We have found that. And we are making efforts there.

And I would say we would be wise to solve problems sooner, before they get more troublesome later. I do think that that is an area that needs more attention in the intelligence community and all other efforts that we make.

Vice Chairman ROCKEFELLER. Thank you, sir.

Admiral Jacoby, I can't imagine that you wouldn't have some comment.

Admiral JACOBY. Senator Rockefeller, you know in past conversations we've talked about sort of the global spread of issues. Cer-

tainly, there's a fertile ground in the Muslim populations in Africa for recruitment to extremist causes. Disaffected youth, the youth bulge, socioeconomic situation, education shortfalls, unemployment and so forth make inviting recruiting targets. And obviously, as we look at the Madrid bombing and some of the things that have happened, particularly the North African crescent is an area of concern.

Sir, we take the Africa situation seriously in the sense that we have plussed up our presence in our defense attache offices and will continue to do that with some new initiatives that go in place here in 2005 and 2006.

We view Africa as place that needs to be monitored carefully. Trends need to be carefully described and assessed and that the intelligence assessments reach policymakers in that part of the world as a sense of urgency.

Vice Chairman ROCKEFELLER. I would follow through to both of you that I think we all know that we have an enormous scarcity of resources, of facilities, of capabilities, simply because of what's going on elsewhere. And I hear what you both say. And I hear the sense of urgency behind what you say.

But I also would guess that there's some frustration on your part that we may not have the financial capability or the trained personnel capability to be able to get to those areas to get that intelligence. Those are difficult languages, and it takes, as Director Goss has often said, 5 years to train a good agent.

Director GOSS. I think you've said it well, Senator.

Admiral JACOBY. I agree completely, sir. Absolutely.

Vice Chairman ROCKEFELLER. Thank you, Mr. Chairman.

Chairman ROBERTS. Let me just say that, in reference to the Vice Chairman's concern about the situation in Russia in regards to loose nukes or loose bioweaponry or loose scientists or loose anything in terms of security, that we should give a lot of credit to the Armed Services Committee and its distinguished Chairman, who is sitting over here to my left and everybody's right—Senator Warner—for taking such a strong interest in the CTR program, the Nunn-Lugar program.

And knowing something about that on the Emerging Threats Subcommittee, we learned right away the most important thing is to provide the security. We want to eliminate the stockpiles and we want to safeguard the scientists and make sure they're not, you know, going somewhere else. But we have made some progress, and we have put some conditions and some of our allies need to step up. And the Russians have stepped up. So I'm very hopeful we'll continue to see additional funding and really address that security issue.

Senator Bond.

Senator BOND. Thank you, Mr. Chairman.

Director Mueller, you noted that the third concern was the recruitment of radical American converts. And this is something that I've become increasingly concerned about.

I don't know if you've seen it, but recently, the Freedom House put out a report on Saudi publications on hate ideologies filling American mosques. And as you read through it, you see the hate-

filled language that is officially sponsored by the cultural offices of the embassy of Saudi Arabia.

And mosques supported by the king has admonitions: be dissociated from the infidels; hate them for their religion; leave them; never rely on them; do not admire them; and always oppose them in every way, according to Islamic law.

The list of documents and the list of publications goes on. And it appears that the bargain with the devil they made about 25 years ago, that the Saudi government would support Wahhabism if they stayed out of Saudi Arabia, is coming back to haunt us.

I would ask the question, number one, how serious a threat that is? And I would ask you and Admiral Loy to respond to it.

And also, it seems to me if our doctrine is that a country that harbors terrorists is guilty, what about a country that fosters terrorists within our own country?

Director MUELLER. Well, it certainly, as I think I indicated in my opening remarks, it is an issue—the radicalization of individuals within the United States. And it can be done any number of ways.

We are looking, for instance, at the prison systems, not just the Federal system but, through our 100 joint terrorism task forces, working with State and local law enforcement to address the possibility that radicalization can occur throughout our prison system, as it has in the past in a variety of ways.

Through our joint terrorism task forces, we also understand that persons absolutely have the right to practice religion in whichever way they want. But by the same token——

Senator BOND. That's not the question, Mr. Director. It's what they are——

Director MUELLER. But I'm going to say, on the other hand, we have the obligation to determine and identify those persons who are becoming radicalized and become a threat to the United States.

And through our working with State and local law enforcement, building up our intelligence capacity, working through our joint terrorism task forces, we continuously seek sources and information and intelligence as to those individuals who may become radicalized in a variety of ways.

The last point I would make—and I think others would agree with me—is that there has been a shift in the attitude of Saudi Arabia in the wake of the May 2003 bombings—a substantial shift, and an understanding and a recognition of the threat not only to Saudi Arabia, but to Saudi Arabia's interests around the world from those elements who have been radicalized.

Senator BOND. Thank you, Mr. Director. They noted that these documents were still, as of December 2004, were still in the King Fahd mosque. They're still being handed out.

Admiral Loy, any thoughts about how, from the homeland security standpoint, how dangerous is Saudi Arabia's supplying of this literature?

Admiral LOY. Indeed, Senator Bond, there are three or four points that I would make.

Number one, regardless of the sponsorship, the notions that you are citing in the things that you read are dramatic evidence of the challenge in front of us here, whether it's pure Saudi from the implication of that particular set of materials, or what that line of

logic is as a pervasive notion throughout not only Saudi Arabia, but the rest of the world.

I sit on a couple of joint contact groups with allies—with the Brits, with Canada. And there has been over the last year a growth of an agenda item referring to radicalization as a significant issue that we have to grapple with.

Senator BOND. Admiral Loy, if I may interrupt. I apologize; the light's on—I needed to ask Director Goss, Ms. Rodley and maybe Admiral Jacoby, I think that Southeast Asia is the second front of the war on terrorism.

Director Goss mentioned that. I've recently come back from there. Jemaah Islamiyah, Moro Liberation Front, others, Abu Sayyaf, are posing significant dangers. Singapore, Malaysia and Indonesia have been aggressive.

Number one, I'd like to know whether you think these have become a threat to the U.S. homeland and are our restrictions on U.S. aid—IMET aid—to Indonesian military hurting our ability to work cooperatively with that country?

Mr. Goss.

Director GOSS. On the IMET question, there is no question that—I can't speak specific to the particulars there. Maybe Admiral Jacoby can.

But I will tell you that, in fact, we do have liaison relationships in the war on terror, of course, on a global basis. And they are affected by other matters such as that that you have specifically mentioned.

In this case I can't answer your direct question, but I can tell you there is a relationship, and it's important that we understand that.

The second thing I would tell you is, I think you are right to focus on Southeast Asia. It is an escalating area. We find that the degree of capability to deal with the problem there is the sophistication of dealing with the problem of terrorism there by the governments, the states that are there, is not adequate. Consequently, I would say it is a growth industry, regrettably.

Yes, it is a threat.

Admiral JACOBY. Senator Bond, the key countries in the area are the ones that Director Goss identified—Indonesia, Philippines, Thailand. Two of those countries we've had very longstanding IMET and other interactions and it makes it far easier to work not only with their military forces, but also with their military intelligence, with my counterparts.

The situation in Indonesia is quite different, where the senior officers in that country, particularly in, again, my case, the intelligence area, have not had those kinds of interactions with the U.S. military.

It does create barriers for close interaction and interoperation. And Southeast Asia in general is an area that needs that kind of attention. And I'm going back to my days in the Pacific command as a J–2 to say authoritatively that more needs to be done there, sir.

STATEMENT OF CAROL RODLEY, PRINCIPAL DEPUTY ASSISTANT SECRETARY OF STATE FOR INTELLIGENCE AND RESEARCH

Ms. RODLEY. We really see it the same way as my colleagues have outlined. Indonesia as the main problem.

Chairman ROBERTS. Speak right in the microphone.

Ms. RODLEY. Indonesia has the most serious problem with Jemaah Islamiyah and, to a lesser extent, the Philippines, Thailand and some of the other nations in the region.

This is of particular concern because of Jemaah Islamiyah's affiliation with al-Qa'ida. So the question of targeting U.S. interests is one that we are very concerned about.

[The prepared statement of Hon. Thomas Fingar, Assistant Secretary of State for Intelligence and Research follows:]

PREPARED STATEMENT OF THE HONORABLE THOMAS FINGAR,
ASSISTANT SECRETARY OF STATE FOR INTELLIGENCE AND RESEARCH

Mister Chairman, Members of the Committee. It is an honor to be asked to participate in this important review of threats to our Nation and the challenges they present to the Intelligence Community. INR has taken to heart your admonition to describe the spectrum of threats to the United States and its interests, and to assess the probability, immediacy, and severity of the dangers we face, but I will do so in a way intended to complement the judgments presented by our colleagues in other agencies by focusing on the way threats appear when viewed through the lens of diplomacy.

The subject of this hearing is one on which there is broad consensus in the Intelligence Community. INR concurs with the judgment that terrorism is the single greatest threat to Americans, both at home and abroad, and that the proliferation of weapons of mass destruction (WMD), missiles, and certain types of advanced conventional weapons is a close and dangerous second. We also share most of the other threat judgments presented by our colleagues. But rather than merely echoing their assessments, I will approach the subject reflecting INR's unique perspective and responsibilities as the Secretary of State's in-house intelligence unit.

As Secretary Rice has made clear in recent statements, diplomacy is critical to U.S. efforts to contain, counter, and diminish the threats we face. On February 8 she told her audience in Paris, "We agree on the interwoven threats we face today: terrorism, and proliferation of weapons of mass destruction, and regional conflicts, and failed states, and organized crime." She added that America stands ready to work with other countries in "building an even stronger partnership" to address these threats.

To combat the twin scourges of terrorism and proliferation requires more than just the effective collection of hard to obtain intelligence. At a minimum, it also requires deep understanding of the motivations and objectives of those who resort to terrorism and/or pursue WMD. It also takes sophisticated analysis of all-source information, informed judgments about what we do not know, and detailed knowledge of other countries, cultures, political systems, and the underlying causes of discontent and radicalization. The prerequisites for meeting all these requirements include global coverage, deep analytical expertise, and Intelligence Community commitment to providing policymakers what they need, when they need it, and in a form that they can use day in and day out.

Why are terrorism and proliferation at the top of the threat list? The short and conventional answer is that the normalization of relations with China and demise of the Soviet Union dramatically reduced the danger of nuclear war and eliminated or transformed fundamentally a wide array of associated threats. But the end of the cold war also brought many changes to other aspects of international life, including the erosion of constraints on "client" states, the re-emergence of long repressed political aspirations, and the rise of ethnic and religious hatreds. Former DCI Jim Woolsey described the change as the displacement of a few big dragons by lots of dangerous snakes. But it was, and is, more than that. Globalization and the information revolution have changed expectations and aspirations and made it possible for nations and non-state actors, including individuals, to do things that would have been unthinkable just a few years ago.

One of the many resultant developments has been the emergence of vast differences in coercive capabilities. This, in turn, has exacerbated the dangers of both terrorism and proliferation. The inability of all but a few nations to deter the most powerful countries (including, but not limited to the United States) has reinforced the determination of states that feel threatened (whether justifiably or not) to seek asymmetric solutions to the disparity of power. For some, this means pursuit of WMD and delivery capabilities because they know they have no hope of deterring or defeating the attacks they fear with conventional armaments. Perhaps the clearest illustration of this can be found in DPRK public statements after Operation Iraqi Freedom intended to reassure its public and warn potential adversaries that, unlike Saddam, it had a (nuclear) deterrent; a claim reiterated February 10. Pakistan pursued-and obtained nuclear weapons and delivery systems to compensate for India's vastly superior conventional military power and nuclear weapons.

Terrorism is at the other end of the spectrum of asymmetric responses. State sponsors, most notably Iran, seem implicitly to warn potential enemies that the response to any attack will include resort to terror. They seem to be saying, in effect, "You may be able to defeat us militarily, but you cannot protect all your people, everywhere, all the time." Such a porcupine defense/deterrent posture is an unfortunate, but not irrational response to wide disparities of power. The situation is somewhat analogous for non-state actors frustrated by their inability to achieve their (however reprehensible) goals by other means. Terror and guerrilla warfare are long-standing measures of choice (or last resort) for weak actors confronting a much stronger adversary. The targets vary widely, from established democracies to authoritarian regimes. However, in some cases, terrorists also direct their attacks against those who are seen as responsible for-by imposition or support the actions or existence of the regime they oppose. That appears to be one of the reasons al-Qaida has targeted the United States in Saudi Arabia and terrorists in Iraq have used suicide bombers and improvised explosive devices to attack Iraqis and others supportive of the Iraqi government. The use of terror tactics in liberal democracies is especially problematic because in open societies, self-restraint under the rule of law and commitment to respect human rights and dignity complicate the challenges of mounting an effective response.

Attacking a distant country is difficult, even in the era of globalization, and would-be assailants must choose between difficult, high profile attacks, like those on 9/11, and easier to accomplish, but probably lower impact incidents (like sniper attacks on random individuals or small explosions in crowded public places). We remain vulnerable to both types of terror attack, but arguably we are now less vulnerable to relatively largescale, high profile attacks than we were before 9/11. Nevertheless, it is extremely difficult to penetrate the tight knit groups that are most capable of carrying out such attacks on our country and our people. We have achieved great success in disrupting alQaida, but may be witnessing a repeat of the pattern found in the wars on illegal drugs and organized crime, namely, that we are fighting a "hydra" with robust capabilities of resurgence and replacement of lost operatives. The bottom line is that terrorism remains the most immediate, dangerous, and difficult security challenge facing our country and the international community and is likely to remain so for a long time. Despite the progress we have made, it would be imprudent to become complacent or to lower our guard.

The quest for WMD, missiles (or unmanned aerial vehicles), and advanced conventional arms has become more attractive to, and more feasible for, a small but significant set of State and non-state actors. This poses major challenges to the security of the United States and our friends and allies, but it is important to put this threat in perspective.

Nuclear Threats. The nuclear sword of Damocles that hung over our national existence during the cold war remains largely a concern from a different era. Russia and China still have nuclear weapons (the number is declining in Russia and increasing only modestly in China), but the hostility of the past is no longer a pressing concern and neither threatens to use them against our country. North Korea has produced sufficient fissile material to make a small number of nuclear weapons, but, despite its February 10 statement, there is no evidence that it has produced such weapons and mated them to a missile capable of delivering them to the United States. However, if it has made such weapons, it could reach U.S. allies, our armed forces, and large concentrations of American citizens in Northeast Asia. India and Pakistan have nuclear weapons and the capability to deliver them to targets in the region, but both nations are friends and neither threatens the territory of the United States. Iran seeks, but does not yet have nuclear weapons or missiles capable of reaching the United States. INR's net assessment of the threat to U.S. territory posed by nuclear weapons controlled by Nation states is that it is low and lacks immediacy. But this should not be grounds for complacency. The existence of such

weapons and the means to deliver them constitutes a latent, but deadly threat. Ensuring that it remains latent is a key diplomatic priority.

The so-far theoretical possibility of nuclear weapons falling into the hands of terrorists constitutes a very different type of threat. We have seen no persuasive evidence that al-Qaida has obtained fissile material or ever has had a serious and sustained program to do so. At worst, the group possesses small amounts of radiological material that could be used to fabricate a radiological dispersion device ("dirty bomb"). The only practical way for non-state actors to obtain sufficient fissile material for a nuclear weapon (as opposed to material for a so-called dirty bomb) would be to acquire it on the black market or to steal it from one of the current, want-to-be, or used-to-be nuclear weapons states. The "loose nukes" problem in the former Soviet Union continues to exist but is less acute than it once was, thanks to the Nunn-Lugar cooperative threat reduction program and diligent efforts by Russia to consolidate and protect stockpiles. North Korea's possession of weapons-grade fissile material adds a new layer of danger and uncertainty. There is no convincing evidence that the DPRK has ever sold, given, or even offered to transfer such material to any State or non-state actor, but we cannot assume that it would never do so.

Chemical and Biological Weapons. Despite the diffusion of know-how and dual-use capabilities to an ever-increasing number of countries, the number of states with known or suspected CW programs remains both small and stable. Most of those that possess such weapons or have the capability to produce quantities sufficient to constitute a genuine threat to the United States or Americans (civilian and military) outside our borders are not hostile to us, appreciate the significance of our nuclear and conventional arsenals, and are unlikely to transfer such weapons or capabilities to terrorists. There are nations that might use CW against invading troops, even American forces, on their own territory, but we judge it highly unlikely that Nation states would use CW against the American homeland or specifically target American citizens except as an act of desperation. Terrorists, by contrast, have or could acquire the capability to produce small quantities of chemical agents for use against selected targets or random individuals. We judge the chances of their doing so as moderate to high. One or a few disgruntled individuals or a small terrorist cell could do so in a manner analogous to the 1995 Aurn Shinrikyo sarin gas attack on a Tokyo subway. The severity of such an attack would be small in terms of lethality, but the psychological and political impact would be huge.

The risk posed by Nation states with biological weapons is similar to that for CW; many nations have the capability, but few have programs and even fewer would be tempted to use them against the United States. The danger of acquisition and use by terrorists, however, is far greater. Though hard to handle safely and even harder to deliver effectively, BW agents have the potential to overwhelm response capabilities in specific locations, induce widespread panic, and disrupt ordinary life for a protracted period, with resulting economic and social consequences oλ uncertain magnitude.

Conventional Attack. INR considers the danger of a conventional military attack on the United States or American military, diplomatic, or business facilities abroad to be very low for the simple reason that no State hostile to the United States has the military capability to attack the U.S. with any hope of avoiding massive retaliation and ultimate, probably rapid, annihilation. The only way to reach a different conclusion, it seems to us, is to posit an irrational actor model in which either all key decisionmakers in a hostile country are irrational or there are no systemic constraints on a totally irrational dictator. We judge that such conditions exist nowhere at present and hence that U.S. military might is, and will be, able to deter any such suicidal adventure for the foreseeable future. Here again, ensuring that this situation continues is a major goal of American diplomacy.

A far more dangerous threat is the possibility, even the likelihood, that advanced conventional weapons will be obtained—and used—by terrorists. For example, the danger that groups or individuals antithetical to the United States will obtain MANPADs or advanced explosives is both high and immediate. The number of Americans likely to be killed or maimed in such an attack would be small in comparison with the casualties in a conventional war or nuclear attack, but would be unacceptably large no matter how small the number of casualties and could have a major economic and psychological impact. Attacks on American nationals, whether they are aimed at workers in an American city, American tourists abroad, U.S. diplomatic facilities, U.S. businesses at home or abroad, or U.S. military facilities at home or abroad, are possible and unacceptable. The fact that State Department personnel, family members, and facilities have been frequent targets of attack makes us acutely aware of this danger and determined to do everything possible to thwart it. This determination is magnified severalfold by the fact that it is an important part of the State Department's mission, and the Secretary of State's responsibility,

to protect American citizens everywhere around the globe. We take this responsibility very seriously, and an important part of INR's support to diplomacy involves providing information and insights that contribute directly to the success of this mission.

States of Concern. It has become something of a convention in threat testimony to list a number of countries that, for one reason or another, are judged to warrant special attention from the Intelligence Community. A few countries on this list engage in activities that directly or indirectly threaten American lives (e.g., North Korea's deployment of massive military power close enough to Seoul to put at risk our ally as well as American troops and tens of thousands of American civilians). Most countries on the list do not threaten the United States militarily, but are important to the success of policies to protect and promote other American interests.

Rather than enumerate a long list of countries, I will simply provide a series of generic examples to illustrate the kinds of conditions and concerns germane to diplomatic efforts to protect and advance American interests. The State Department needs good intelligence on some countries primarily because their actions could lead to internal instability that could, in turn, threaten other American interests. Others belong on the list because they do not or cannot prevent the growth and export of narcotics, harbor or assist terrorist groups, have leaders who make anti-American pronouncements, or have conditions conducive to the rise of extremist movements. Still others illicitly traffic in persons, weapons, conflict diamonds, or other commodities; control critical energy resources; or have fragile political institutions, large and dynamic economies, or any of myriad other attributes.

What states on this long and varied list have in common is the capacity to affect American interests and the efficacy of U.S. foreign, economic, and security policy. Most do not and will not "threaten" the United States in the way that we were once threatened by the Soviet Union and the Warsaw Pact, but something, or many things, about them pose challenges and/or opportunities for American diplomacy. The problems of failing states and the tremendous drain on resources in developing countries from AIDS and other pandemics, environmental stress, and corruption affect our ability to partner with allies and friends to meet humanitarian needs in the interest of promoting stability and democracy. This, in turn, poses challenges and requirements for the Intelligence Community that extend far beyond the collection and analysis of information germane to the suppression of terrorism and limiting the spread of WMD, delivery systems, and advanced conventional weapons. Meeting these challenges requires global coverage, deep expertise, extensive collaboration, and, above all, acceptance of the idea that the mission of the Intelligence Community demands and entails more than collecting and interpreting covertly acquired information on a relatively small number of narrowly defined threats. Focusing on known threats and concerns is necessary, but could prove to be very dangerous if we are not equally vigilant in trying to anticipate unknowns and surprises.

Intelligence is, or should be, about more than addressing "threats." The Intelligence Community has been justifiably criticized for serious failings and shortcomings, but we should not lose sight of what we do well and must continue to do well. For example, America's unrivaled military preeminence, demonstrated so dramatically in our elimination of the Taliban regime in Afghanistan and the destruction of Saddam's regime in Iraq, is inextricably linked to the capabilities and accomplishments of our Intelligence Community. Intelligence collection, analytic tradecraft, insights gained through years of experience, and close ties among collectors, analysts, weapons designers, military planners, and troops on the ground are all and equally critical to the military successes we have achieved, the predominance we enjoy, and the fact that conventional military threats to our Nation and our citizens are low and almost certain to remain so for many years. Preserving this State of affairs will be neither automatic nor easy, but our efforts and the allocation of resources to do so must not foreclose equally committed efforts to address other threats and challenges.

Terrorism and proliferation are at the top of every agency's list of threats, and the Intelligence Community is committing substantial effort and resources to provide the intelligence support required to contain and reduce those dangers. In part, this requires and involves penetration of highly restricted and suspicious organizations and secure systems of communication, including sophisticated measures to hide financial transactions, obscure relationships, and deceive human and technical collectors. But collection is only one of many essential factors in the equation. To place the intelligence we collect in context, to distinguish between what is true and useful and what is not, and to develop strategies to detect and disrupt activities inimical to American interests requires expert analysts and information on a very wide array of critical variables. Stated another way, it is not possible to identify, anticipate, understand, and disrupt terrorists and proliferatitios without broad and

deep understanding of the countries, cultures, contexts, social networks, economic systems, and political arenas in which they spawn, develop, and operate. Without broad and deep expertise and information that goes far beyond what we can or should collect through clandestine means, we will not be able to judge accurately the information we collect, and will ultimately be reduced to reliance on lucky guesses and chance discoveries. That isn't good enough. We can and must do better.

Senator BOND. Thank you. Thank you, Mr. Chairman. I apologize to my colleagues.

Chairman ROBERTS. Senator Feinstein.

Senator FEINSTEIN. Thank you very much, Mr. Chairman.

Let me begin by thanking each of you. I think those of you that particularly head large departments, it is a most difficult time to give your service. And I just want you to know how much I appreciate it. So, thank you very much.

I view a worldwide threat to be our borders. And I'd like to explain that a little bit. Let me begin by quoting the Homeland Security statement today, Admiral Loy. On page four of your statement: "Recent information from ongoing investigations, detentions, and emerging threat streams strongly suggest that al-Qa'ida has considered using the southwest border to infiltrate the United States. Several al-Qa'ida leaders believe operatives can pay their way into the country through Mexico and also believe illegal entry is more advantageous than legal entry for operational security reasons."

I think that is a very important statement, particularly when you consider the fact that a half-a-million other-than-Mexican intrusions have been made on our borders since 2000. Specifically, with respect to the southwest border, in 2003 there were 30,147 other-than-Mexican intrusions. The next year, 2004, which is the latest year that we have figures for, there were 44,617. That's a 48 percent increase.

Now, let me take you to a hearing—because I sit on the Judiciary Immigration Subcommittee—and a response by Mr. Hutchinson to Senator Grassley's questions in February 2004. This was a hearing held about a year ago. And let me read an answer.

"At present, DHS has no specific policy regarding OTMs apprehended at the southern border. While OTMs, as well as Mexicans, are permitted to withdraw their applications for admission and can be returned voluntarily to their country of nationality, as a practical matter this option is not readily available for them, as it is for Mexicans, whose government will accept them back into the Mexican territory. Thus, when apprehended, OTMs are routinely placed in removal proceedings under Immigration and Nationality Act 240. It is not practical to detain all non-criminal OTMs during immigration proceedings. And thus, most are released. A majority of OTMs later fail to appear for their immigration proceedings and simply disappear into the United States.

"DHS is reviewing the possibility of extending its expedited removal authority and means of addressing this problem. DHS is also considering a variety of alternatives to detention, especially for asylum seekers."

Now, I've looked at the statistics for each country. And the so-called countries of concern—Syria, Iran, others—the numbers are up of penetrations through our southwest border. Clearly we are deficient in a mechanism to deal with these.

Could you please comment and could you please indicate what actions are being taken? I view this as a very serious situation.

Admiral LOY. Thank you, Senator Feinstein. And, indeed, we view it in exactly the same way you do, as a very serious situation.

There have been a number of initiatives over the course of the last year, many of which I know you're familiar with. For example, the opportunity for deep repatriation of people back into—not just across the border where the recidivism rate is that they'll be back, coming our direction that night or the next night.

The whole notion of being able to take the repatriation decision and take Mexican nationals, illegal aliens back to——

Senator FEINSTEIN. I'm not talking about—none of these are Mexican nationals. These are all OTMs—other-than-Mexicans—44,000 OTMs came across the southwest border last year.

Admiral LOY. Yes, ma'am. I'm just trying to array a set of tools that could be potentially of use, not only in Mexico, but wherever the OTMs might be from.

The challenge here is a lengthy border, as you well know. We are introducing technology along that border that'll substitute for what has historically been a very human-intensive effort along the border, to make a difference in terms of comings and goings.

So, US-VISIT, the notion of using UAVs on the border as plugs between those portals of entry that we have worked so hard to harden, if you will. But the entry-exit system that has been now deployed by the Department of Homeland Security after, I would offer, 20 years or so of effort on the part of INS beforehand in failed efforts to establish some kind of a legitimate, biometrically based entry-exit system into the country, that we have some confidence in in terms of our abilities to say who is here and who is not, and what are we going to do about those who we can track and find.

Senator FEINSTEIN. Let me have a little discussion on this. Because essentially, there is no detention for these people. They don't show up for their hearings and they disappear. So we really don't know who comes into this country illegally over that southwest border.

I have two cases that the FBI was involved in, one actually in Michigan, where the gentleman was clearly a terrorist. He pled guilty. He got 6 months. This is a big problem in the United States. And I really don't think that the mechanical aspect of it is going to solve it. You're not detaining these people. They're released, essentially.

Admiral LOY. Well, there certainly is a prioritization process to those with any degree of a connection against the national terrorism database that has now been forged for us to be able to bounce names against. So, to the degree we are releasing because of the resource implications attendant to keeping them and bedding them and detaining them until resolution can come of their individual cases.

Those without any apparent criminal and/or terrorist connection are obviously those that are on the high end of the release order and the low end of the detention order.

Senator FEINSTEIN. Can you give us a number of how many are being detained?

Admiral LOY. I don't have that with me at the moment, but I'll be happy to provide it to you.

Senator FEINSTEIN. I would appreciate it. Out of the 44,000 that came in in 2004, how many are detained. I appreciate that.

Admiral LOY. We'll provide that.

Senator FEINSTEIN. Thank you, Mr. Chairman.

Chairman ROBERTS. Senator Chambliss.

Senator CHAMBLISS. Thank you, Mr. Chairman.

Director Goss, because of our longstanding relationship going back to our House days, you know how keen my interest has been in this area of information sharing. I was very pleased to hear you, as well as Director Mueller, say that things are improving. But at the same time, you both recognize we still have a long way to go.

Donnie Harrelson, the Sheriff of Criss County, Georgia, happened to be in the back a little earlier, and I visited with him for a minute. He was keenly interested in a number of things that were being said. And I told him that we really can't let this issue of information sharing rest until his office and every other local law enforcement office has the information in real time that they need to help us win this war on terrorism domestically. So, I appreciate the continued effort of everybody at the table on this issue, but obviously especially you two.

Director Goss and Admiral Jacoby, there was a report on Fox News this morning in which it stated that the Iranians have alleged that an aerial vehicle of some sort fired a missile and it did not explode, but it was fired in the area of a nuclear facility owned by the Iranians.

Would either of you care to comment on the information that has come out of Iran this morning relative to that issue?

Director GOSS. Senator, thank you for your comments about vertical integration of information and your patience on letting us get the technology and our architecture, our enterprise, together on that. There is progress since we last talked, and that's good news.

On the subject of Iran, I know nothing in my official position. What I do know is, I think, from press reports that something did fall out of the sky and came down somewhat near Bushehr, their ongoing building of their nuclear power plant in that area.

I also heard a subsequent report—and I have no idea whether I'm spreading a rumor or not—that it was a gas tank that fell off an aircraft and exploded. And I have no idea whether that's true or not. It just came into my ear.

Admiral JACOBY. Senator Chambliss, I have no knowledge of the report or any incidents involving Iran.

Senator CHAMBLISS. Director Mueller, I have had the opportunity to visit with your joint terrorism task force folks in Atlanta and intend to do so again in the very near future. And I will tell you, I am very impressed by the work that's ongoing with that operation.

Every time I meet with them, I am told by some of your FBI agents in the field, as well as other local law enforcement officers, of the importance of the PATRIOT Act, and their ability to fight terrorism as well as fight crime with the tools that they have under the PATRIOT Act.

Now, as you know, the PATRIOT Act, or certain provisions of it, are going to be expiring at the end of this year. Would you care

to comment on what your thoughts are relative to the reauthorization of those provisions that are set to expire, and how useful the PATRIOT Act has been to your organization in fighting crime and fighting terrorism?

Director MUELLER. Let me just start off by saying that the provisions of the PATRIOT Act are indispensable to the protection of the American public against further terrorist attacks.

And the heartland of the bill that is so important—and it's not just important to the FBI, but it's important to the CIA, the DIA and others in the intelligence community, as well as State and local law enforcement—is the breaking down of walls that inhibited our ability to share information across our agencies and across our disciplines and across our programs. And the safety of the United States depends on the ability of all of us together to be able to accumulate the information, share the information.

And I don't mean just in pushing, but having access, equal access to the information, and having the opportunity to act on that information and all the information, whether it be act within the United States, in a city, in a town, in a State or nationally, or overseas, by having access to information that may have been collected within the United States or outside the United States.

And the PATRIOT Act has been instrumental in breaking down those walls and enabling us to do it. It has given us new authorities. That has given us the ability to obtain information that will allow us to identify persons who present a threat against the United States with adequate predication of their interest and motivation in so doing.

It has given us access to records that we previously did not have, but often are instrumental pieces of a puzzle that'll give us a broader vision, a broader view of the intentions of an individual or of a group of individuals in the United States.

And I know myself and others who live day in and day out trying to prevent terrorist attacks will be here before Congress on a number of occasions, asking Congress to please continue to let us have those tools to protect the American public.

Senator CHAMBLISS. Thank you. Thank you, Mr. Chairman.

Chairman ROBERTS. Senator Levin.

Senator LEVIN. Thank you, Mr. Chairman.

Mr. Goss, we were given information on an unclassified basis in January of 2002, as follows. This is a CIA assessment. "We assess that North Korea has produced enough plutonium for at least one, and possibly two, nuclear weapons." I'm wondering, Director, if you could give us the current CIA assessment.

Director GOSS. I'm honestly not sure whether or not the assessment is classified that we have. But our assessment is that they have a greater capability than that assessment. In other words, it has increased since then.

I would also point out there are other agencies that are making assessments, and there is a range. And I think that the range we're fairly comfortable on—and I know that is classified. Be happy to share that with you in closed session.

Senator LEVIN. If you also could tell us for the record if there's any unclassified numbers you can give us—for the record, if you can do that. I'm not asking——

Director GOSS. Senator, I will.

Senator LEVIN. If you can give us numbers the way that number was given. And also, Director Goss, this is for you.

The 9/11 Commission included a number of recommendations for realigning the Executive Branch, including the following. "Lead responsibility for directing and executing paramilitary operations, whether clandestine or covert, should shift to the Defense Department." Do you agree?

Director GOSS. I recall the issue very well.

Senator LEVIN. Just briefly, do you agree with that?

Director GOSS. I do not agree with that conclusion. We have studied it, and the Secretary of Defense and I have a memo which I anticipate signing today.

Senator LEVIN. Is that going to be public?

Director GOSS. Certainly the conclusion of it will be.

Senator LEVIN. I think as much public as you can make, obviously.

Director GOSS. It's in everybody's interest to know, I think, how we are dividing up the responsibility.

Senator LEVIN. I think it is.

Director GOSS. I can tell you we spent a lot of time looking at this. And the Secretary feels that he has capabilities that are important, and I agree. And I feel I have capabilities that are important, and he agrees. There's not a lot of disagreement on this. We just didn't come out the same place the 9/11 Commission did.

Senator LEVIN. Thank you, Director.

I understand that your CIA's Inspector General's report on treatment of detainees by members of the intelligence community is somewhere in the pipeline. Can you tell us where it is?

Director GOSS. Yes, sir.

Senator LEVIN. When is it going to be available?

Director GOSS. The IG, or the inspector general of the agency, has indeed got all of the complaints and the referral on that matter in hand. As you know, it's an independent position. I have checked.

There is one report that was ordered by my predecessor, which has come back, which had 10 recommendations or so in it. About, I think, eight of those have been done.

We are now into the process of looking at some of the specific cases that have been brought to the IG. I cannot tell you what his timetable is, but I'm sure he would be very happy to tell you. I am assured that the work is ongoing, as it should be appropriately.

Senator LEVIN. Well, if he'd be happy to tell us, wouldn't he be happy to tell you?

Director GOSS. Sure.

Senator LEVIN. Well, what is the timetable? I mean, is there a time?

Director GOSS. I haven't asked him what day he's going to finish all these cases.

Senator LEVIN. Or a month?

Director GOSS. As soon as they are through. I know one case has been dismissed. I know one case has been prosecuted. You've read about it in the paper, in North Carolina. know there are still a bunch of other cases. What I can't tell you is how many more might come in the door.

Senator LEVIN. OK. Thank you.

Director Mueller, this is for you. It relates also to the interrogation question. The FBI documents which were released under a FOIA request include e-mails from FBI agents expressing their deep concerns, that during late 2002 and mid–2003, overly aggressive and coercive interrogation techniques were being used by the Defense Department people at Guantanamo's detention facility which "differed drastically from the FBI's authorized practices."

Those memos described the Department of Defense's methods as, quote: "Torture techniques," expressed disbelief over the military's interviews, telling their colleagues back in Washington—this is in the FBI—that "you won't believe it."

The FBI agents also described heated exchanges and battles with the commanding generals at Guantanamo over the Department of Defense's interrogation techniques, which FBI agents "not only advised against, but questioned in terms of their effectiveness." Incidents described included detainees being chained hand and foot in fetal positions, no chair, food or water for long periods, ended up defecating on themselves. One detainee apparently had been literally pulling his own hair out throughout the night.

Another major concern of the FBI agents present at Guantanamo was that the Defense Department interrogators were impersonating FBI agents in order to gain intelligence. FBI agents were deeply worried that should detainees ever publicly report their treatment at Guantanamo the FBI would be left "holding the bag," because it would be appear falsely that "those torture techniques were done by FBI interrogators."

Those documents make clear that the FBI was so concerned about the Department of Defense's interrogation techniques that it issued guidance to FBI agents at Guantanamo to stand clear and to keep away from those techniques when the DoD took control of interrogation.

I assume that because of the serious and extensive objections that were lodged by FBI agents against those techniques, and particularly given the heated discussions at which your personnel were present and engaged in, that you or your senior advisers were aware of the concerns of those members of your staff.

And I'm just wondering—this is my question—did you raise those concerns with either senior officials at the Department of Defense, the Attorney General or the head of the criminal division at the Justice Department, or higher-ups in the Administration, including the National Security Council?

Director MUELLER. Senator, I know that those concerns were raised with the Department of Defense by persons within the FBI. At least some of those were, at least three incidents early-on.

Certainly after the issues were raised about Abu Ghraib there were additional memoranda that were generated as a result of an inquiry to the field that you may have been alluding to there. Those also have been brought to the attention of the military.

I will also say that our inspector general is doing a review of when the information came in and what happened to that information once it came into the FBI.

Senator LEVIN. You personally did not raise those concerns with senior officials at the Department of Defense or with the Attorney General or the head of the criminal division?

Director MUELLER. I was not aware of those concerns until May of 2004.

Let me just be precise on that, Senator. I was not aware of the concerns that you raised, that you allude to there, in Guantanamo until May of 2004.

Senator LEVIN. Thank you. Thank you, Mr. Chairman.

Senator LEVIN. Thank you.

Chairman ROBERTS. Senator Snowe.

STATEMENT OF THE HONORABLE OLYMPIA J. SNOWE, U.S. SENATOR FROM MAINE

Senator SNOWE. Thank you, Mr. Chairman. I want to welcome all of our panelists here today.

Director Goss, just to follow up on one of the questions that the Chairman raised with respect to A.Q. Khan, there's no question that he masterminded a far-reaching, wide-ranging, global in scope operation in dispersing nuclear information activities and technology.

Have we pressed the Pakistani government to allow a U.S. representative to directly have access to A.Q. Khan for questioning to determine the extent of his network of elicit nuclear activities?

PREPARED STATEMENT OF THE HONORABLE OLYMPIA J. SNOWE, U.S. SENATOR FROM MAINE

Mr. Chairman, thank you again for holding this vital hearing that will give us an opportunity to examine the threats currently arrayed against our Nation as well as a look at those threats that may endanger our society in the future. Identifying these threats each year is crucial to our ability to gauge our progress in defeating or mitigating those threats and to understanding this Committee's role in providing the oversight and resources required by the Intelligence Community to help defeat those who wish us harm.

This hearing will also give us an opportunity to examine the progress of the changes initiated since passing the Intelligence Community reform in the last Congress and the confirmation of the new Director of Central Intelligence. But, in the end, it is the current and emerging threats to the Nation that drives our investments in, and the development of priorities for, the Intelligence Community's collection and analytic capabilities. I intend to look at a wide spectrum of these threat scenarios—from the threat posed by nuclear-capable terrorists to the future emergence of a regional peer-competitor, as well as to our abilities to protect the homeland.

I also want to thank Mr. Goss, Director of Central Intelligence and Mr. Mueller of the FBI for once again appearing before the Committee to describe to us their view of the world and how their respective agencies are facing the many challenges before them.

I especially want to acknowledge Admiral James Loy's appearance here today. Although he has announced his departure from public life later this spring, he remains committed to the nation's defense, as he has been for his entire career, and has come before us today to describe the Department of Homeland Security's efforts to counter the threats arrayed against the homeland. On a personal note, as Chair of the Senate's Subcommittee on Oceans, Fisheries and Coast Guard, I was able to work closely with Admiral Loy when he was Commandant of the Coast Guard. His charge to protect the Nation has always been a part of his personal code of honor and he has been unwavering in accomplishing his mission. For that and his many years of public service, I thank him—the Nation is not only grateful, but safer, for his loyalty and dedication.

I would be remiss if I didn't comment directly about the dedication and professionalism of the thousands of Americans who make up our Intelligence Community.

Each day, across this country and around the world, they labor, often without recognition, to keep this country safe from harm. It is their vigilance upon which we rely to give us the forewarning necessary to counter the many dangers present in our world. Although it is impossible to directly express our deep appreciation for their efforts, I charge our witnesses to relay our eternal gratitude to those who serve America so well.

It has been an extremely challenging year for the Intelligence Community; one in which we saw two major reports detailing the actions and failures of our collective intelligence community to provide national decisionmakers with the timely and quality intelligence they must have to prepare America for the threats faced by the Nation and the need to go to war. On the heels of those reports, we in Congress undertook the largest revamping of the intelligence community since its inception with the 1947 National Security Act. This self-examination and correction is a hallmark of our democracy and will serve to make us stronger. It is my fervent hope that the professionals of the community see this reorganization as an opportunity to renew their dedication and take on the challenges to strengthen their craft. In these perilous times, the Nation needs them now more than ever.

We on this Committee have spent a great deal of the past 2 years poring over the intelligence provided to decisionmakers before the commencement of Operation Iraqi Freedom and, of course, we all learned many things and reached many conclusions. In my analysis of that information, I became more and more convinced that while Saddam's nuclear programs may have been defunct, our Nation continues to face the very real threat of nuclear terrorism.

Terrorists are known to be seeking nuclear technologies and have already displayed a proclivity for catastrophic destruction on a massive scale. For terrorists, attacking a U.S. city with a nuclear device would likely be their "dream come true." In the February 6 *Washington Post*, Steve Coll, author of "Ghost Wars," notes that Osama bin Laden's inspiration, repeatedly cited in his writings and interviews, is the American atomic bombing of Hiroshima and Nagasaki, which he says shocked Japan's fading imperial government into a surrender it might not otherwise have contemplated. Bin Laden has said several times that he is seeking to acquire and use nuclear weapons not only because it is "God's will," but because he wants to do to American foreign policy what the United States did to Japanese imperial surrender policy.

I intend to focus my work on the Committee on this specific threat to the United States because I believe it is time for us to look closely at how we can prevent and deter such a threat. I am also acutely aware from my work on the Commerce Committee in the area of transportation, maritime and port security that we must look to the seas as a very likely path of introduction of such a weapon into the United States. The 9/11 Commission found that "Opportunities to do harm are as great, or greater, in maritime or surface transportation (compared to commercial aviation)."

Recognizing these vulnerabilities, I included a number of provisions and acted as a conferee to the Maritime Transportation Security Act signed into law in 2002. One of my provisions included a requirement that foreign shippers send their cargo manifest before arriving at a U.S. port so the Department of Homeland Security can more efficiently evaluate individual container shipments for risks of terrorism. I have also held several port security hearings at the Subcommittee on Oceans, Fisheries and Coast Guard and will continue to do so because I do not believe we are anywhere near finished with fully securing our maritime borders.

That is why I was encouraged by the President's announcement in December of his Maritime Security Policy National Security/Homeland Security Presidential Directive, which outlined his vision for a fully coordinated U.S. Government effort to protect U.S. interests in the maritime domain. The directive charges the Department of Defense and the Department of Homeland Security with the alignment of all U.S. Government maritime security programs and initiatives into a comprehensive and cohesive national effort involving appropriate Federal, State, local and private sector entities.

This move comes at a critical time. As we sit here right now, the Department of Defense is proceeding with the 2005 Base Realignment and Closure (BRAC) process, which I continue to believe is the wrong thing to do while we are engaged in a global war on terrorism. We must ensure that in the DoD's drive to meet an arbitrary 25 percent reduction figure in infrastructure, we do no harm. For example, Brunswick Naval Air Station on the coast of my home State of Maine is home to one of four remaining maritime patrol bases remaining in the Navy and, in fact, possesses the only remaining fully capable active runways in the entire Northeast.

While many say that the maritime patrol community, whose chief mission is anti-submarine warfare, is not relevant in the post-cold war world, the community has reinvented itself as the warfighting commander's premiere manned, long-range in-

telligence, surveillance and reconnaissance (ISR) platform and is performing admirably in direct support of Operation Enduring Freedom and Operation Iraqi Freedom.

But this community also has a role in the President's maritime security policy. We have been talking to the Coast Guard and it is clear that if we want to be able to conduct ISR operations against inbound maritime traffic farther than 200 miles from our shores, the maritime patrol community offers a ready and proven capability. These points are made eloquently in a white paper written by retired Navy Captain Ralph Dean who concludes that optimum basing for maritime interdiction assets is as important as the assets themselves. We must, therefore, carefully factor in future requirements for maritime interdiction before closing any of the maritime patrol bases, which are located in the four corners of the continental U.S.—Maine, Florida, Washington state, and California.

The use of conventional forces to interdict the asymmetric threats facing the Nation leads me to my final point. The Nation cannot afford to develop tunnel-vision when it comes to the threat we face. Just as the U.S. failed to adequately counter the developing threat of terrorism as we focused solely on the cold war threat, I am concerned that we do not now focus solely on terrorism and ignore the growing likelihood of a regional peer competitor in the Pacific region. Like many, I am alarmed by the rapid and unprecedented buildup of naval forces, particularly destroyers and submarines, by the Chinese People's Liberation Army Navy.

Last month members of the House Armed Services Committee visited China and came away deeply concerned. Representative Randy Forbes said, "We're seeing China really make huge moves in the area of its navy. . .There's no question our Navy is the best in the world. . .but at some point, sheer numbers start to matter."

So I am doubly concerned when the Navy sends Congress a budget that radically cuts the number of next generation destroyers and submarines to be built by the Navy. I believe that in the future we will need conventional "blue-water" ships to maintain our global presence in the Northern and Western Pacific. I look forward to hearing from VADM Jacoby as to the Defense Intelligence Agency's assessment of the Chinese naval threat and what we are doing now to counter that threat before we wake up one morning to yet another "new normalcy," just as we did on September 12, 2001.

I look forward to hearing the testimony of our witnesses and working with them as part of this Committee to ensure that our intelligence community has the resources and structure it needs to meet the national security challenges we face today and in the future.

Thank you.

Director GOSS. Senator Snowe, I want to be very careful how I answer your question. I think my definition of "pressed" and yours would be the same. And I would say yes.

I can tell you that there is continuous attention to this matter. And I believe that is being done with the necessary urgency and fortitude, to make sure our interests are completely understood.

Senator SNOWE. So, could you characterize the cooperation on the part of the Pakistani government, sharing information?

Director GOSS. Yes.

Senator SNOWE. I think it is disconcerting. I'm sure you saw the article in *Time Magazine* recently citing a source close to the Khan research laboratories in Islamabad. And he's quoted as saying, "even though its head has been removed, Khan's illicit network of supplies and middlemen is still out there."

Director GOSS. Senator, in about 2 minutes in a private conversation, I think I could satisfy your answers to these questions.

Let me just simply say, there is an understanding that A.Q. Khan enjoyed a certain amount of celebrity status in his country because he was the man who brought them the bomb, which was very critical to that culture and their national pride and so forth.

It has been a difficult prospect. And understanding the problem there, have to dealing with it, is useful in negotiating our interests, which are to get all the information possible.

I think that those discussions are understood and appropriate steps by the right people are taking place. I can be more specific in private.

Senator SNOWE. I appreciate that.

Admiral Loy, I'm sure you're familiar with this report from the inspector general of the Department of Homeland Security regarding the visa waiver program and the use of stolen passports from the visa waiver countries.

And it's pretty troubling and disconcerting the extent to which aliens have applied for admissions into the United States with stolen passports from these specific countries and have been admitted, even when information has been submitted to the lookout system, all the more disconcerting, I think, when you consider—and I think we all agree—the greatest threat to this country is having terrorists have access to nuclear weapons or the materials to manufacture them.

And this report indicates "aliens applying for admission to the United States using stolen passports have little reason to fear being caught and are usually admitted. Our analysis showed that it only made a small difference whether the stolen passports were posted in the lookout system."

They reviewed two groups. Of the first group, 79 of the 98 aliens attempting entry were admitted. The second group had lookouts posted for their stolen passports prior to their attempted entries. And from the second group, 57 out of the 78 aliens who attempted entry were admitted.

Thirty-three of these admissions occurred after September 11, 2001. And then 136 successful entries using stolen passports were allowed.

I mean, obviously, this is significant and disturbing, to say the least, that obviously we haven't made much headway with respect to this issue regarding stolen passports. And when you think that worldwide there are 10 million stolen passports, it only takes one to gain admission into the United States.

You know, when you think about the fact on June 6, 2001, according to this report, 708 blank passports were stolen from the visa waiver program. The IG reported that this was significant because the passports were stolen in a city that also was the location of the al-Qa'ida cell that played a significant role in providing financial and logistical support for the September 11th terrorists.

It's interesting as well because there is little attempt by law enforcement officials to follow up and to try to locate these individuals, even when they have learned—even when officials have learned—that they have come into this country illegally.

So, one, what are we doing to investigate these activities of these aliens that have used stolen passports? What are we doing to determine their whereabouts? And what are we doing to improve our ability to locate, investigate and remove these individuals from the United States, who have stolen passports to gain entry?

Admiral LOY. Thank you, Senator Snowe. It's a very serious issue. The ICE agency is following up dramatically as a result not just of the IG's investigation but, rather, of their recognition of this, I'll call it, chink in the armor, so to speak.

We must recall that, of course, over the course of a couple of hundred years of our country's openness to people coming to our borders, our exit-entry control system attendant to those borders was, frankly, very weak.

The fact that the last year-and-a-half that we have established US-VISIT as an entry-exit control system, that we have engaged internationally to try to use Interpol as a database storage for stolen passport information, so that there's a database that can be used internationally, not just by folks of concern coming to the United States, but crossing any borders anywhere.

The visa waiver program in and of itself now is required—any folks coming into our country from visa waiver countries go through US-VISIT, and we begin to gain the biometric value of the fingerprints and the facial imagery that we capture as they come into our country each time they enter.

We are conducting reviews of the visa waiver countries as we speak. There are 25 of the 27 countries being reviewed, as the Congress biannually, with a report due back to provide you a solid status report on the visa waiver countries as it relates to the issue that you're describing.

Furthermore, that review process always has the opportunity for sanctions attendant to it, as to whether or not one stays in the visa waiver program at the other end of the day.

There have been rather dramatic, public reflections of both Germany and France and other countries having this nightmarish problem of not tens or twenties, but literally thousands of their brand-new, machine-readable passport blanks finding their way into the status that you were describing. So it is a significant international issue that we're trying to fight on all those fronts.

Senator SNOWE. Well, it's clear that we need to do something very expeditiously.

Admiral LOY. Including the enforcement.

Senator SNOWE. I think it's a huge challenge and the countries better be cooperating in that regard.

Admiral LOY. Exactly.

Senator SNOWE. Thank you, Mr. Chairman.

Chairman ROBERTS. Senator Wyden.

Senator WYDEN. Thank you, Mr. Chairman and gentlemen. Sorry, we've got multiple hearings going on this morning and I didn't get to hear all of your testimony.

But I did understand that several of you made the point that information sharing is improving. And I will tell you that I'm still concerned that the walls that have prevented information sharing still have not been brought down. And to some extent what has happened, the pre-9/11 walls that prevent information sharing seem to have been replaced with a new set of walls that prevent information sharing. And I want to give you an example that revolves around the area that you all talked about, the National Counterterrorism Center, NCTC, where you all feel things have gotten better.

Now, our Committee has been told that, while information can be shared among those who work at the center, an analyst has to go out and seek approval before sharing information that may be

of value with the home agency, and the approval may or may not be granted and it's sort of a bureaucratic shuffle to get it done.

My question would be to you, Director Goss. Are you aware of the problem? And if so, how do you believe it ought to be addressed?

This is something that our Committee has heard about now several times. And it sort of caught my attention when you all were talking about information sharing improving.

Director Goss, your response?

Director GOSS. Yes, I'd be very happy to, Senator. Thank you.

I do believe that the across-the-board information sharing is improved. There are still areas—and this is one of them.

Senator WYDEN. I want to make sure I got that you say this is an area that you will still be willing to work with us on.

Director GOSS. Oh, absolutely. This is not finished business yet.

We have the question of how do you protect an individual agency's sources and methods? How do you get assurance for that agency when they are making a contribution?

And the question of how we use either TAGINTs or tearlines, or how we make this available, it's easier if you're just talking about a customer. But if you're talking about an analyst that wants to go further in and probe further and perhaps do tasking, then you come to the questions of some of the things we're trying to use, like co-location, getting the analysts and the collectors to talk together, changing things with agencies, setting up different rules.

Part of that is going to be the business of the new DNI. As you know, the NCTC reports to the DNI. And the NCTC is now run very, very effectively, I would say, but on an acting basis, by John Brennan.

They have absorbed the TTIC into the NCTC. And I think they've gone just about as far down the road as they can go without stepping on the prerogatives of a new DNI, whose main function, in my view, is going to have to be sorting out the authorities and the interface between the DNI's job and responsibilities and the individual agencies—and those interfaces between the 15 agencies in the community.

Because until you do that and make those lines clear, the question of sharing proprietary—and excuse me for using the word, but it does fit—information is going to be difficult, because everybody is charged with preserving their sources and methods.

Senator WYDEN. I think what concerns me is that there are a finite number of people working the terrorism issue for the entire intelligence community. They all hold security clearances. They're all trained.

And it just seems to me that these analysts ought to have access to all the information that can help our side. And I would like to talk about this with you all further, talk about it more, perhaps, in a private session.

But it seemed to me, what we ought to have is the equivalent of a terrorism analyst program—a special terrorism analyst program—that would allow all of these analysts access to all the same data.

And until we get there, we're still going to be trying to break down these walls. And time is short. We'll talk about it some more,

but I think, Mr. Director, your answer is constructive. The acknowledgment that there is more work to do is what I was interested in hearing.

It just seems to me there's only so many people in this community. Let's make sure they all can get access to the same kind of information. And there's an awful lot of shuffling going on, just with NCTC. And I'm just not going to take this further, but I saw Bob Mueller nod, and I consider that constructive, as well.

The second area that I'd like to touch on involves accountability. If there's one thing my constituents are frustrated about as it relates to government is the absence of accountability. And still after 9/11, I keep looking for anybody who lost a job, was demoted, was reprimanded—any kind of consequences—and I can't find any. I can't find any anywhere.

And my question would be to you, Director Goss, in that you all apparently have a report from the Inspector General, as a result of input from this Committee, the Joint Inquiry on the terrorist attacks, where there was clear interest in the Inspector General conducting a review to determine if any CIA officials ought to actually be held accountable for the mistakes that led to the attacks. And I'm trying to figure out where this Inspector General report is. I gather there are just layers and layers of review.

But where are we on this Inspector General report? What can you tell us today? When are we going to get it on this Committee, so that we can get serious about some accountability?

Director GOSS. Senator, thank you. You will get the IG report as soon as it is finished. I've made the same pledge yesterday to HPSCI. It was commissioned, I think, by Congress, and you'll get it. And the IG is independent.

Now, as for where is it right now, the IG came to me shortly after I came in and said that this matter was under review and he would be presenting it shortly to me, for the next step, because there is a process, apparently, in how this works.

And I asked him a very simple question. I said, if you are naming names, are you giving those names the opportunity to express their views? And it turned out that in the process he had not taken that option. I suggested to him that in the interest of what I would just simply call American fair play, if you're going to start bandying people's names about, you might let them know what it is you're saying about them. And he agreed. I did not instruct him to do that, please understand. We just had a discussion about how this process would unfold. This is somewhat new.

And so I understand that he has done that. And individuals have been advised of what this report says about them, on a confidential basis. I also understand that some of these individuals have hired attorneys because they wish to, for whatever reason, have that kind of advice. When attorneys come into the issue like this, I understand that the timing becomes a little uncertain of when matters will be concluded.

I do not feel it appropriate for me to demand a deadline at this point, since the process has elements of due process in it. And I view that the IG is capable of making the decisions of when he's ready to present that to me. That has not happened at this point.

When he does, I have already got two staffers I've selected, who are in the process or I suspect have probably read the report. So we will be able, when it comes to my level, as the Director of the Central Intelligence Agency, to decide whether or not it is appropriate to convene boards in the agency, in-house, to deal with accountability or not. And that is apparently what my responsibility will be.

Either way, this Committee and the other Oversight Committee—the House Oversight Committee—will get the IG's report. And it is understood, it will be classified.

Senator WYDEN. Do I have time for one additional question, Mr. Chairman?

Chairman ROBERTS. I think Senator Mikulski has been waiting very patiently throughout the whole hearing. And if we have time for a second round, I would be delighted to recognize the Senator. And I don't mean to pick on him, in that most Senators have gone red.

I think I'll probably leave that comment alone.

The patient, but always accommodating, Senator from Maryland.

Senator MIKULSKI. Patient. Yes, a signature characteristic of myself, well known to all.

[Laughter.]

Senator MIKULSKI. Good morning, and thank you really for what you do everyday. I think all of us appreciate the fact that the job of everybody here is to prevent predatory attacks against the homeland, against U.S. assets abroad, against our troops, and even to help predatory attacks against allies.

I'm going to focus on the issue of terrorism and want to come back to this whole issue of how we have gotten better at connecting the dots and focus really on threats to our ports.

So these are really questions for Directors Mueller, Goss, and Admiral Loy. There's considerable concern that sea-based or shipborne terrorist attacks are big concerns and big possibilities. Many analysts are concerned about the security of U.S. ports, foreign ports, but in my case, like Baltimore and other coastal Senators.

So my question is: Of the various scenarios, which do we fear attacks on our ports? Do we fear nuclear weapons being smuggled in and detonated at a U.S. port? And what are we doing about it? And how did the three of you work together?

And Admiral Loy, of course, we know you from your Coast Guard days, and you've adapted to a new transportation mode pretty quick. But you see where we are. So there's Goss, you know, looking at the world. You know, Loy's got Mr. Homeland Security. And there's Mueller, and he's got the domestic whatever. So where are we on the threat to the ports, and what are we doing to prevent the threat? And how do you all coordinate this information so that Governors, and mayors, and the people can feel pretty good about it?

Director GOSS. Thank you, Senator. I'll start.

I will tell you that my normal day starts in the company of these two gentlemen. And matters of this urgency are discussed between us. But, not only that, we have close working relationships between our agencies. And it is well understood, the danger of which you speak, properly.

In terms of our part, from the national foreign intelligence program, obviously, leaning overseas and getting all the information we can to stop it over there and to get information before something's put on a ship, or to understand a plot, is very, very important. I would point out—somebody can correct the statistic—but it's a very high percentage of success, perhaps 95 percent, of all drug interdictions come from good tips from information, not from random searches.

But you have to do the gates-guns-guards approach domestically to take care of the ports. And you have to do the information approach. Am I satisfied they're as plugged in as they can be? Yes, under the circumstances that we have.

Now, with the DHS and with the FBI, law enforcement people, people with new responsibilities dealing with homeland security, and our very clear understand that this is part of the target for our operatives overseas, I think we have done as good as we can do, in terms of understanding information that's critical.

Senator MIKULSKI. I appreciate that the three of you meet, but I'm talking about all the way down, are we really communicating?

Director GOSS. I think it goes pretty far down for us.

Director MUELLER. For us, in every city that there's a port, there's a Joint Terrorism Task Force with a specific responsibility to work closely with the elements of the port to exchange information and provide what can be done to enhance the port security. In several of the ports around the country, we have—particularly where there's substantial ferry traffic, for instance—we have done intelligence analyses of vulnerabilities of the ferry services.

Each port has a little different mixture of the type of shipping that comes in. And consequently, the Joint Terrorism Task Forces, working with the Coast Guard and other elements, work closely with State and local law enforcement as well as the other Federal components, to come up with a plan to assure that we have the intelligence that's necessary to focus on the threat of a potential attack. And then, if there's an attack, how we are going to respond to it.

And perhaps I can turn that over to Admiral Loy to pick up on.

Admiral LOY. Thank you, Senator Mikulski.

The information flow into this challenge is as was just described by Director Goss and Director Mueller. At the other end, I would offer that the chair I was sitting in on 9/11 was still in uniform as the Commandant of the Coast Guard. And, frankly, we spent the rest of the time that I was in that great service focusing on domestic maritime strategy—domestic maritime security strategy.

We also recognized that it was enormously important to see that this was an international challenge immediately, because all of those 9 million containers a year, 20,000 a day, that find their way to Baltimore and many other ports come from overseas. And so one of the first things we did was literally take a delegation to the International Maritime Organization to start a process which has become a standard-setting effort for international commerce as it relates to facilities, crews, ships that ply the waters of the United States, to meet those international standards.

Second, there have been excellent resource plus-ups attendant to the Coast Guard's capability to shift gears from emphasizing what

it has always been able to emphasize as an array of responsibilities it has for the Nation and focus on port security in this particular time of need.

I think one of the greatest strengths of that service is its agility to reshape its focus on what Nation needs it to focus on now. And it certainly has done so over the course of these last 3 years.

We have also recognized the legitimacy through port security grants and Operation Safe Commerce. The requirements that we have to look down the supply chain, literally from the point of origin to the point of destination, with a sense of transparency all the way through that, in order to see and be able to apply the insights we gain from the intelligence community as to what we should be doing operationally in those various responsibilities.

The notion of pushing our borders out so that they don't become the first portal that we look at things under concern about, the Container Security Initiative, as I mentioned in my opening comments, is now alive and well in 34 different ports where customs agents, side by each with their host nation counterparts, are watching the stuffing of those boxes, the sealing of those boxes, as it relates to cargo security.

One of the most dramatic initiatives that we had already underway for what then Vern Clark and I, as the Chief of Naval Operations, viewed as an asymmetric array of threats, which shifted focus to the terrorism piece of that asymmetric array after 9/11, had already been underway in Suitland with a joint effort, with respect to intelligence reviews that the two sea-going services of this Nation jointly conduct there day after day after day.

That has developed into two initiatives today. One of them attended to something I termed maritime domain awareness and has become almost a term of art in this look that the two services take. With NORTHCOM's responsibility reaching 500 miles out to sea on the Pacific side and literally almost 1,700 miles to sea on the Atlantic side, we have joined forces, the Navy and the Coast Guard, to truly understand what's going on and how do we assure that we know what's going on in the domain we're responsible for.

Senator MIKULSKI. Let me come back.

First of all, this was really, I think, very helpful, and I hope enlightening to the Committee. I know my time's up. But number one, how real is this threat?

And number two, Admiral Loy, homeland security is the ultimate user of the intelligence, the ultimate customer, of course, along with the FBI. But, you know, you're Coast Guard. You're Customs. That's the battle line.

Admiral LOY. We hold the bag. Yes, ma'am.

Senator MIKULSKI. Yes. One, how real is this threat? And number two, do you really feel that what has been described is really working well?

Admiral LOY. The gathering and the sharing of the information, this is, I think, working extraordinarily well in this particular domain. I think, to go back to the Chairman's commentary about information access as opposed to information pushing and the comments that the Vice Chairman made attendant to that, are absolutely right on point.

We discussed, though, there just two operatives. You talked about the analyst and you talked about the collector. And I would offer that the operator is the other absolutely crucial ingredient to keep in that algorithm. The requirements that the operator can express to the collector and the analyst go a long way to figuring out the workload of those people on any given day, any given week, for any given purpose or project.

So I would ask you to have the operators articulate their requirements, those things that they're going to be able to use properly to do the work they're required to do. Let the analysts and the collectors then get about that business to meet those operators' requirements.

Senator MIKULSKI. Threat?

Admiral LOY. The threat is as real here. We have the same kind of exercise program to think our way through the nightmare scenarios on the maritime sector, as in any other sector. Ports represent that place where it all comes together. Ninety-five percent of what comes and goes to this country comes and goes by the water. So the port complexes are clearly a targeted area for the terrorists.

Senator MIKULSKI. Mr. Chairman, I presumed my time was up. That was a lengthy conversation, but I think really is crucial, because that's where it all comes together.

Chairman ROBERTS. As usual, the Senator raised an important point. Has the Senator finished her comments?

Senator MIKULSKI. My time is up.

Chairman ROBERTS. The distinguished Chairman of the Senate Armed Services Committee.

Senator WARNER. I thank you, Mr. Chairman and the Ranking Member. We've had a good hearing. I'm sorry I had to step out for a moment.

Sixty years ago this month, at age 17, I started my very modest and inauspicious military career. And I had over a half century of the privilege of being associated with the men and women of the United States military. And this afternoon, like so many of our colleagues, I go to Arlington for the burial of a brave Marine who lost his life in Iraq.

As I sit through these ceremonies quietly, the thought always occurred to me, "Senator, have you failed to do anything in your official capacity either to equip or train this individual or to provide him the intelligence, or his superiors the intelligence, which could have prevented this death?"

There is an issue here, I say to my distinguished Chairman and Ranking Member and colleagues on the Committee, which I think we've got to address, both in my Committee and in this Committee. And that is the manner in which we gain intelligence from those that are captured, either on the battlefield or in other areas.

There has been a good deal written, and I draw the attention of my colleagues to an article today in *The New York Times* entitled, "CIA is Seen as Seeking New Role on Detainees." And so my question to you is as follows.

America has always been a Nation that follows the rule of law, and we must preserve that. And the Geneva Convention, as such, is a part of our body of law. But we recognize other nations have

other laws, traditions, whatever. And there could well be means by which they gain intelligence which we can't, following the rule of law. And I'm not suggesting we deviate from the rule of law.

But when an individual is apprehended in Iraq, should we turn him over to the Iraqis, who may have a different system, and from that individual we gain information that not only preserves the opportunity to protect our coalition forces, but indeed the terrible and tragic killing of so many Iraqi citizens and their own security forces.

I think largely this issue has to be addressed in closed session. But I wonder, Mr. Director, to what extent you can talk about what your hope is in this area to gain the maximum intelligence that we need to not only bring to, hopefully, a successful conclusion of the Iraqi campaign, but other campaigns on other fronts and, at the same time, carefully preserve the traditions of this country by following the rule of law.

And most specifically, what should we do in dealing with other countries in terms of sharing the burdens of captivity and interrogation of a witness or a captive or whatever we may have in our possession? And then I'll ask the Department of State, Ms. Rodley, to give the views of State on that.

Director GOSS. Thank you, Mr. Senator.

The subject is of critical importance to us. You are correct to point out that we are dealing in a life-and-death business, and you are correct to point out that interrogation is a mainstream of information. Having enough professional interrogators operating the proper way, that would be within the rule of law, and professional interrogators will tell you that torture is not something they would wish to have, because it doesn't work. There are better way to deal with captives.

So I don't think there is any inconsistency with the idea of professional interrogation of combatants, whether they're conventional or unconventional, taken off the field of hostility and brought into our captivity, being subject to a professional interrogation. I do not think that's an impossible job.

The question of who does it and under what circumstances does get us into some legalities. I'm not a lawyer, an attorney. And I will obviously be guided by what they say. But that is not going to be a deterrent to a professional program. It's just going to affect the mode a little bit.

Clearly, as Americans, we are concerned with legality, the rule of law. We are concerned with human rights because we are compassionate human beings, and what we stand for is what we're fighting for. And we're not going to abrogate that.

We have an immediacy of protection of forces and protection of innocent lives in the interrogation process. We do not want to forego that opportunity. Nor would we ask another country to do something that we would not do ourselves as a cute way of end-running our commitment to the law and decency.

I believe that we have most of that in hand. There are some parts of that that I cannot answer with you yet that are sort of down-the-road pieces of it that I need to talk to you about in closed session.

But if you asked me today, is interrogation vitally important to saving lives, and disrupting terrorists, and protecting our forces, the answer is unequivocal. Yes.

If you are asking me today if we are handling interrogation within the proper norms and bounds, the answer is yes. If you are asking me today if I would like to get more information from some of our captives that I still think have information we would like to have, the answer is yes. And if you asked me would I like to have more captives tomorrow to interrogate, the answer is yes.

Senator WARNER. Let's take it to one last subject. When you're given the option that you could transfer this prisoner to another nation, recognizing that nation employs methods different than we, how would deal with that?

Director GOSS. I would require safeguards, if that captive were going back, either as a non-interrogee or as an interrogee. If that individual is being returned to a nation, a judgment should be made that nothing beyond, I would say, due process punishment, if that is deserved, would happen to that individual, even though they may not have the same standards in that nation.

As you know, many nations will claim their citizens back. And we have a responsibility of trying to ensure that they are properly treated. And we try and do the best we can to guarantee that. But, of course, once they're out of their control, there's only so much we can do. But we do have an accountability program for those situations.

Senator WARNER. Thank you.

Chairman ROBERTS. Senator Bayh.

Senator WARNER. I hadn't finished.

Chairman ROBERTS. I beg your pardon.

Senator WARNER. Could the witness from the Department of State give their perspective from their department?

Chairman ROBERTS. Certainly.

Ms. RODLEY. Thank you, Senator Warner.

One of our key policy goals in Iraq, obviously, has been to build and to build up institutions in Iraq—government institutions, government services—that will adhere to the rule of law. This is a long-term process. Mr. Goss's agency has been involved in this project with us in the stand-up of the new Iraqi intelligence service.

It's a long-term process, obviously. But we are, of course, heartened by the results of the election in Iraq. And we are following closely the formation of the new government there. And we are hopeful that the new government in Iraq will be a government that respects the rule of law, and that the Iraqi people, who suffered horribly for a long time under a brutal dictatorship, won't be subject to the kind of abuses that routinely went on under Saddam Hussein.

So I wouldn't automatically assume that detainees turned over to the Iraqi services now would suffer the same fate that has been the case very commonly in the past.

Senator WARNER. But, Mr. Chairman, if I could just ask a question for the record, such that they can, I guess, given my time's up, have to answer for the record.

But I'm following carefully initiatives by Secretary of Defense Rumsfeld as he begins to augment his gathering of intelligence which he deems essential. And, frankly, thus far, in my examination, he's acting within the guidelines of the law, including the newest law that passed the Congress, in establishing a greater ability to collect, I think, largely tactical intelligence.

And if the Director would provide for the record his views—because I'm sure you're following this—as to whether or not you're of the mind that he is acting within the bounds of the law and not in any way conflict with the objections of the new law in establishing these units.

The distinguished Chairman and Ranking Member have begun to look at this. We both, our Committees, have had hearings or briefings on this subject. And it's a matter of active consideration here in the Senate side.

Director GOSS. If I'm permitted——

Senator WARNER. You'll have to take it for the record, because I don't want to interfere.

Director GOSS. I'm very happy to answer if the time is permitted.

Chairman ROBERTS. Let me just say that the distinguished Chairman has asked the question that I was going to ask in reference to the encroachment stories that we have been seeing, both in reference to the FBI and the Department of Defense, in augmenting their intelligence operations in cooperation with you. You don't look encroached upon as of this morning.

And that we have had a hearing with Admiral Jacoby and with Dr. Cambone in the Intelligence Committee about Title 10, Title 50, and the legalities involved. They have, in fact, kept the Committee informed through the staff and through this hearing, but I do think that if you could submit that answer to the record, you know, for the Chairman, I think it would be very helpful, because I think this is a subject we're all interested in.

Senator WARNER. Thank you, Mr. Chairman.

Director GOSS. Mr. Chairman, Mr. Chairman, I am completely comfortable with where we are in terms of forward-leaning efforts by all of the elements in the intelligence community to do the best they can with the missions that we have been assigned. It is quite clear to me that there has been a lot of speculation and RUMINT and so forth, and comment in the paper, which is unfounded or badly founded.

The truth is that I believe that the efforts that the Department of Defense is trying to undertake are entirely appropriate. They are looking forward to the best ways to get the information they need to accomplish their objectives with the maximum protection for their warfighters. I think that is excellent.

What it involves is some coordination overseas and some understanding about who's doing what where. I go to the analogy that the leader of our country team in any overseas situation is the Ambassador, the chief of mission, that the person who is normally in charge of intelligence, all intelligence activities, is the representative of the Central Intelligence Agency.

That does mean there's no other intelligence going on except under the Central Intelligence Agency's immediate direction. It means it's coordinated there. And I believe that we understand

that. Those details, in some cases, yet to be worked out, because there is forward-leaning, which we have not seen forward, which is entirely appropriate.

I can say on the domestic front exactly the same thing. There have been a lot of stories about who is doing what. There is no question that the intelligence community has the experience to do—it's the National Foreign Intelligence Program overseas. There's also no question that occasionally agencies like the FBI need to be overseas doing things that they do very well in pursuit of their role in counterterrorism. We ask that it be coordinated.

Equally, I think that the FBI wants to be assured, as do I, that we are not usurping our authorities in the domestic homeland. We all know Americans do not spy on Americans. And that is our absolute pledge. It is equally true, however, we need some support. And we do have a support base that we use in the United States. It is critical that we keep that coordinated with Director Mueller.

These are questions of working out details. Perhaps a DNI would have done it faster than we are doing it. But I frankly think we're doing it quite well, considering we've got 15 agencies doing very intense things that we haven't done before.

I realize that the DCI, which is one of my titles, is an endangered species. But I will be handing off my thoughts to the DNI. And my thoughts are forward-leaning by all agencies is good, and we can coordinate it and make it work.

Senator WARNER. Mr. Chairman, I'm very impressed by the responses you've given to both of my questions. I wish you well, and we're fortunate you've taken on this task.

Director GOSS. Thank you, sir.

Senator WARNER. You could have been basking in that sunny clime of Florida.

Director GOSS. Thank you, Senator.

Chairman ROBERTS. Senator Bayh.

Senator BAYH. Senator Warner, sometimes the heat in Washington is just as warm.

Thank you very much, all of you, for your service to our country. I really do appreciate it. These are issues of profound importance, the resolution to which is often not clear. I wouldn't be surprised if all of you didn't lose a significant amount of sleep over your service to our country and dealing with what you're dealing with, so I thank you for that.

I also apologize, Mr. Chairman, to you and the panel for having to shuttle back and forth. Alan Greenspan, Chairman Greenspan, was testifying before the Banking Committee today, so we are trying to simultaneously deal with our Nation's economic security and prosperity and our physical security here. So I apologize for my absence.

Let me begin by asking a question that involves credibility. And I want to make very clear that it doesn't involve personal credibility. No one would question any of your personal credibility. But I think we do have a national credibility problem.

And so what I want to ask specifically is, for the Americans watching us today and hearing about assessments involving Iran and North Korea and what is maybe going on there that could be threatening our country, what has improved over the last couple of

years since the assessments about weapons of mass destruction in Iraq that would give greater assurance to the American people that what we're hearing today is accurate?

Without getting into obviously classified specifics, have our collection capabilities improved significantly? Have our analytical capabilities improved significantly? Why should people place, you know, credibility behind what we're saying here today, given the history with regard to WMD in Iraq?

Director GOSS. That's actually the perfect question, and that's what we do. That's, I think, why we all go to work.

How do we take what we were using and make it better and more appropriate? And I think I can report back that we have more collectors, better technology being properly applied and more focused in the application, more analysts who understand the language, who understand the pitfalls of group-think, more systems that put this together to make the information come out more timely, more flexibility in our systems to deal with problems as they pop up—and the nature of our enemy is pop-up, quite often—and a greater understanding of each other's problems.

We have all walked a little in everybody else's shoes, and I think we see it a little differently. And I think that that's been a helpful exercise. We need to get on with the architecture of what the community is going to look like, and we need to make sure that each unique contribution of each of the elements of the community is provided for in a way that it is still unique and adding value to the total product.

I think that we are moving well.

Senator BAYH. Are we encouraging contrarian analysis? You mentioned group-think.

Director GOSS. Indeed, we are. And we're publishing it, too, right on the same page.

Senator BAYH. Any of the rest of you care to comment about capabilities having improved? If not, that's OK, too.

Admiral JACOBY. I'd like to just echo the Director's words and talk about a couple of other things, processes, processes that you bring, you know, the different views together, processes that have made more sourcing of information available as we go to community products, and in my agency, a tremendous emphasis on training and retraining all the way through the senior levels to make sure that we are reinforcing good analytical, logical source utilization kinds of capabilities that are available to us.

Senator BAYH. Thank you.

Yes, Director Mueller.

Director MUELLER. I would say our capabilities have dramatically increased. We had a little bit over 1,300 counterterrorism agents before September 11th. We now have 3,000-plus. We've established an intelligence directorate which has a total complement of 3,787. Of those, 438 are agents, 490 translators, 2,273 analysts.

We have, in each of our field offices, a field intelligence group that was not there before. Our ability to obtain the intelligence, analyze the intelligence, and getting the intelligence to the operators has improved dramatically since September 11th.

Senator BAYH. One of the things I think we've all realized is that in some of these areas there is just an irreducible level of ambi-

guity. And we try and minimize that, but in some of these areas it's still there. And so a certain level of humility in reaching conclusions is, I think, in order in all of our parts.

Let me ask you about North Korea and what you assess to be the likely reaction to our current strategy in North Korea and the role that China might play. But let me back up for a second. At least in 2000, with regard to their plutonium effort, it seemed to have been in stasis. Now they may have been cheating on the uranium side, but cameras were in place. Those have been removed. Inspectors were in place. Those have been removed.

There were published reports that plutonium has been reprocessed and possibly devices have been created. There are even published reports that perhaps in some other areas they may have proliferated. This is not a happy course of events over the last several years, and at least the initial strategy, which seemed to be threaten and ignore, does not seem to have worked too well.

Now we currently have a strategy of engagement through the 6-party talks, trying to encourage the neighbors to take charge of their own neighborhood. My question is: What do you assess the North Koreans' likely response to be to our current sort of sticks and carrots approach, number one? And number two, might a cynic not think that China, which is in a very good position to be helpful on this, that there might be an interest there in not resolving this problem, because as long as North Korea is there and of concern to us, that gives them leverage over us in a variety of other areas.

So, my question is, what do you assess the likely response of North Korea to our current approach? And second, how do you assess the role that China will play in trying to reach a positive conclusion?

Director GOSS. I'm going to try and avoid a policy comment.

My view is that we are seeing what is the traditional bluster diplomacy by North Korea, trying to threaten something terrible and get something concrete back. They're dealing with nothing to get something, and they do it very effectively. And this has been their MO, in my view.

As to their response, I think that their responses are predictable. They are going to continue to do what they want to do. Their number-one goal is survivability of the regime. And that is where they are going to go. And whatever it takes, that's what they'll do. How ridiculous they look on the world stage does not seem to bother them.

Senator BAYH. Forgive me for interrupting, Director. Is there anything, in your estimation, or anybody else's estimation, that could convince them that the survival of their regime—since that's their top priority—is inconsistent with the creation and possession of nuclear weapons? They seem to have concluded that those two things have to go hand-in-hand. What, in your estimation, could lead them to a different point of view?

Director GOSS. I do not know the answer to that question. I just simply don't have that information. I could make a guess and say for them to be relevant, they feel that they have to be in the nuclear club.

There is another aspect that's practical. That's the way they make their money. Their bread-and-butter money is selling this stuff, proliferating.

The Chinese response that you ask, I think the Chinese understand they have got a very troublesome child right there in the nest of the family, and they can't go anywhere. The real estate's not going to change. They've got to deal with the problem.

They have border problems, refugee problems, all kinds of things. I think the Chinese are genuinely interested in not having this be a worse problem. Now, I'm not going to practice diplomacy. I'm going to yield to the Department of State. Much of that was my personal view, not an informed intelligence response.

Senator BAYH. Thank you, Director.

Ms. RODLEY. I'm just going to pick up on that point about the Chinese. We agree with that assessment, that the Chinese are genuinely interested and have concluded that it is in their interest to resolve the problem with North Korea. We don't see any indications that they think it is somehow in their interest in dealing with us to have North Korea continue to be a problem.

Senator BAYH. But they seemed to be in denial for such a long time, I'm glad they finally found religion on this issue.

Just two quick things, just very, very quickly.

Hizbollah, you report their capabilities in terms of striking U.S. interests, if provoked. Should we assume that if it was ever in our national—if we ever felt compelled to act against Iran, that might be the sort of triggering event that we would have to anticipate, Hizbollah taking some sort of action against us?

Director GOSS. I would certainly recommend that any policymaker considering that take that calculation.

Senator BAYH. My final question is with regard to FARC, kind of looking out beyond the horizon. Any assessment by any of you about—obviously, they have capabilities of striking our interests in Colombia. Are you at all concerned about their potential for striking us here in the homeland?

Director GOSS. Well, I used to represent southwest Florida. And I have perhaps a different view than others. But I do feel there is an immediacy to making sure we understand what is going on there. There are, obviously, dialog and communications going on between the countries. That means there can be between the bad players. And I think it's very important for our law enforcement people to be absolutely on top of that. And, as far as I know, they are.

Senator BAYH. Director Mueller.

Director MUELLER. We have not seen, I do not believe, any indications or preparations for FARC to launch an attack in the United States. However, there are ties between individuals associated with FARC and persons in the United States. And they're something we have to keep an eye on.

Senator BAYH. Thank you. Again, I appreciate your service. Thank you all.

Chairman ROBERTS. Let me just say that, in reference to Senator Bayh's comment, if Kim Jong-Il would suddenly get religion, having been to North Korea and trying to deal with that regime in regards to the famine—and they always have a famine, but it was

a more severe famine several years ago—he is the religion. He is a deity in his own mind, and the people believe that, as was his father. So it's a little difficult.

And I would agree with Director Goss. That's the only card he has to play on the world stage, and they're going to play it. And they're going to continue. I still think our best opportunity is to do exactly what the Director said with China in the 6-party talks. But I have no illusions of all of a sudden him getting a light bulb to go off. They don't have any light bulbs, by the way, in North Korea.

And following on your statement, I'd like to ask a question about Iran. And by your statement, I mean Senator Bayh.

Admiral Jacoby, your written statement says that Iran is likely continuing nuclear weapon-related endeavors, is devoting significant resources to its WMD programs, and that, unless constrained by a nuclear non-proliferation agreement, Tehran will probably have the ability to produce a weapon early in the next decade.

Director Goss, your statement notes that the CIA is concerned about the dual-use nature of the technology that could also be used to achieve a nuclear weapon.

Ms. Rodley, your statement notes that Iran seeks, but does not yet have, any nuclear weapons.

It sounds like to me you all agree that, just like Iraq before 2004, Iran has troubling dual-use nuclear capabilities. What I'm interested in, and both the Vice Chairman and I want to get into capabilities and whether or not we have the capabilities to determine some intelligence analysis on intent. As far as Iran's intent to build a nuclear weapon, it sounds like there might be a difference of opinion between you three. I'm not suggesting that, but at least that might be the case.

I would ask all three of you to give us your assessment of Iran's intent, to characterize your confidence in that judgment, and if you feel that should be better handled in a classified section, I certainly appreciate it.

Director GOSS. Mr. Chairman, I would limit my answer. I think there is something I would say that is obvious. There are other players in the neighborhood that are very concerned that also have views about what Iran is up to. And it's important that we understand what that might lead to.

I believe that, having watched the pride of some countries in acquiring the world-stage status of having nuclear weapons and what that has meant for nationalism and leadership, is that it becomes almost a piece of the holy grail for a small country that otherwise might be victimized living in a dangerous neighborhood to have a nuclear weapon.

So, in my view, there is an inclination, a very strong inclination, by the conservative leadership, present conservative leadership of Iran to make sure that they can live up to the same levels as some of their neighboring countries. And some of those neighboring countries—indeed, Pakistan comes to mind—have the bomb.

Chairman ROBERTS. Admiral Jacoby.

Admiral JACOBY. I would join Director Goss, in terms of the intent part. We did some work recently looking at the direction that threats were going. And they are going away from conventional force-on-force confrontation strategy with the United States toward

terrorism on one end and nuclear weapons and not only the status, but the perceived deterrent value, that comes with them.

So I would join the Director, in terms of intent in Iran, and would also say that we're engaged in a hard look at sequentially nuclear programs or suspected nuclear programs in various countries. Iran is next on our agenda, and I believe that our look and the Committee's look will probably coincide. And we look forward to working that together.

Chairman ROBERTS. Ms. Rodley.

Ms. RODLEY. I don't disagree with anything that's been said. I would merely add that another element that makes this harder to get at is the advantage of ambiguity when it comes to nuclear programs.

In a sense, the Iranians don't necessarily have to have a successful nuclear program in order to have the deterrent value. They merely have to convince us, others and their neighbors that they do. This is a lesson that hasn't been lost on them, and it merely complicates both the collection and the analysis on this issue.

Chairman ROBERTS. I thank all three of you for your comment.

I'm enjoying the red light—I'm now a member of the red light club. Have patience, Senator Wyden.

This is a parochial question, but it's really not. It's a national question. Tommy Thompson, the former secretary of HHS, left and said his was worried about the Nation's food supply. And all of us who are privileged to represent States who are involved in agriculture were asked time and time again—I just heard it again on the radio as of yesterday. I'm not sure why Tommy said that.

But, at any rate, Admiral Loy, can you tell me how the Department of Homeland Security views the threat of what we call agroterrorism. The Emerging Threats Subcommittee of the Armed Services Committee 4 or 5 years ago got into this subject area, knowing how serious it could be, but not many people were really thinking about it.

They had an exercise, or one of the many exercises that has been held, called Crimson Sky. Six States were infected by foot-and-mouth with an attack from Iraq. Devastating results happened, utter chaos. We lost our markets. The herds had to be destroyed. People panicked in urban areas. Our food supply was—and I'm not talking about 1 year. I'm talking several years.

So are those efforts now really being coordinated well with other agencies, specifically the Department of Agriculture? Are you getting the intelligence you need? What kind of a priority are you putting on this? This is sort of the Mikulski port/Roberts agriculture question.

Admiral JACOBY. Yes, sir, Mr. Chairman.

Without a doubt, the Homeland Security Presidential Directive 7 first of all directs the Secretary of Homeland Security to be the collaborate effort to pull together the critical infrastructure protection of our Nation writ large. One of the economic sectors cited in that directive is the food sector. And so that has caused the Secretary of Homeland Security to challenge that designated lead-sector agency in the Department of Agriculture to develop a plan attendant to becoming a piece of this puzzle that will be the additive

piece for food, as it relates to the whole critical infrastructure protection of our Nation.

So there has been very good work undertaken with the Department of Agriculture in agricultural operations, the meat-poultry-eggs world, and in the HHS/FDA world responsible, if you will, for the rest of the food production and distribution chain that they're responsible for.

We're at a point where this critical national infrastructure protection plan, the base plan, has been completed and submitted to the White House. Each of these sector plans, we have taken stock—we at the Department have taken stock of how we felt their original plan submission met the specifications that were outlined in HSPD–7 and have offered that commentary back to, in this case, the Secretary of Agriculture, with a bit of a challenge to go back to the drawing boards a bit and resubmit such that the thresholds are reached with what we think are the right concerns to allow not only that to be a free-standing sector and plan attended to food protection for our country.

Chairman ROBERTS. OK. When did you send that over?

Admiral JACOBY. That's back just before the holidays, sir.

Chairman ROBERTS. So that would be under the auspices of the new Secretary of Agriculture, obviously. How many people do you have on board in regards to homeland security that either are on loan from, or consulting with, or are a regular employee that are dealing with this? I know that's a tough question to ask you right here. I think I know the answer. There's one, at least that I know of.

Admiral JACOBY. There's one as a detailee, if you will, into the Department in this business.

Chairman ROBERTS. Yes.

Admiral JACOBY. And, of course, we've got those elements from Agriculture that came into the border portal validation process.

Chairman ROBERTS. Yes.

Admiral JACOBY. But the effort is to allow the Agriculture Secretary to take the lead with respect to developing these plans for our country and make sure that they fit well, because we could have 13 perfect plans, and I'm convinced that it's the interdependencies between and among them that are the real challenge.

Chairman ROBERTS. It's a very hard thing to develop a contingency plan to try to mitigate this. Well, OK, I'll stop at that point, because I've already gone way over my time. But I need to visit with you and the new Director about this as we can determine.

Chairman ROBERTS. Senator Rockefeller.

Vice Chairman ROCKEFELLER. Director Goss, just a very specific and one short question. Before the election, we went up a color.

Director GOSS. I'm sorry?

Vice Chairman ROCKEFELLER. On imminent threat, we went up from yellow to orange, and nothing happened. And there has been no talk or consideration, at least that I'm aware of, of similar elevations since then. I'm wondering if, to the extent that you're involved with it, sir, to the extent that Homeland Security, FBI is involved with it, has there been attempt to go back and review the nature of that intelligence and whether or not it was a psychological move or whether—I don't mean by that political. I mean

psychological simply as a warning to others—or whether it was, in fact, justified. Has there been an effort to go back and re-look at that intelligence?

Director GOSS. Senator, in part, the answer's yes. I don't know all of the things that have been looked at. But part of that, and again, I'm not—that's not my decision area. We provide the information. Part of that, I think, was an assessment of the Usama bin Ladin statement that came out, that there was a question, was that trying to interfere, and some of the questions of propaganda began to really take shape. Exactly how that figured into the decisions that were made by others on raising the elevation, I don't know.

Have we gone back and taken a look? The answer is yes. And I'll tell you why. One of the things that Senator Bayh was pointing out—I should have answered and I neglected to—is that we have learned the difference between a worst-case scenario and a most-likely scenario. We need to be very careful how we need to present these things so people are hearing things not as worst-case scenarios, but as most-likely scenarios, if that's what we believe.

We find that, when the chatter level goes up—that's an expression we like to use because it sort of covers up what we're really talking about—but it means there's something to be tuned into. All of our sensors out there, the system is blinking red, all of those kinds of statements that we've heard. What it means is that we're getting a huge flow of information.

The problem is, how much of that is just wishful thinking and how much of it is real planning? That is a very hard question to make a judgment on. We are going back, as part of our process of how do we get our product better, how do we make sure our customer understands what we're saying.

And that process is very clearly part of the overall process that Senator Bayh was asking about. Are we attending to correcting not only the collection piece, but the analytical piece, including operators, incidentally, when they're available?

Director MUELLER. I think there has been an effort to go back and look at the—well, we continuously review the threat posture day in and day out. And I convinced, given the information we had at the time, that we made the right decision, in terms of the actions we took, given the intelligence at the time.

Subsequent to that there has been further development in that intelligence that may call into question at least some of that intelligence. But you also have to reflect upon the fact that we had al-Hindi, we had the surveillance documents, the Prudential, the stock exchange, a number of things back in this time prior to the election, along with intelligence that indicated that we can expect a threat or an attack in that period before the election.

As I indicated in my opening statement remarks, we undertook substantial efforts to assure that such an attack did not take place. We will never know whether those efforts, our efforts, the efforts of the CIA, the efforts of DHS, the efforts of our counterparts overseas, were effective in reducing or removing that threat of an attack before the elections.

But in reflecting upon what we knew at the time, I believe that we took the right steps. That doesn't mean that we can't do it bet-

ter the next time, but I'm comfortable with the decision that was made back then.

Admiral LOY. Sir, I think that's a very good capture of the time. One thing I would offer is that, over the last 2 years and certainly in the last year, where we are with respect to capability, where we are with respect to stature of an interagency security plan that we keep track of day after day after day, I would offer that today's yellow is probably much closer to yesterday's orange as it relates to the constancy of capability that is there 24 by 7/365 around our country.

So we have simply grown and matured, both as a brand-new department trying to coordinate and collaborate on many of these things. And the absolute value of some of the contributions that are being made by many yield an attitude, if you will, that has the country sort of at a level significantly stronger than it ever was before.

That offers us a chance to keep from the going up and down road, so to speak, when the net evaluation of all the players at a SVTC or a series of weekly and daily meetings that we conduct, rates the flow going by as not being "worthy" of adjusting the homeland security advisory system to a greater level.

I think the country should take great assurance that the level of capability attendant to these things is significantly higher day after day after day. And that simply is a result of us learning lessons going back from each of the experiences of up-and-down that we've undertaken and then ratcheting up, as appropriate, the prevention, the protection, and the response capabilities of the Nation across the board.

Vice Chairman ROCKEFELLER. I thank you.

Chairman ROBERTS. Let me just say—and Senator Wyden, I'll have to buy you lunch or something or, for that matter, probably all of you, but we don't need to get in any food depravation here. And so I'll try to make this quick. I hope there's a look-back on this.

Admiral LOY. Indeed, there is.

Chairman ROBERTS. The same people, same table, same threat, no consensus before our Committee in regards to access to information. That was the problem. Same representatives testifying before us that you're in charge of, that do this on a day-to-day basis. And then, 30 days later, a lot of questions about the credibility of the sources.

Now, if you're going to err, you're going to err on the side of safety, for goodness sakes. I know that. And if you take certain steps, you can't come back. We even had one Senator leave this place as a result of this. He did come back. But I'm saying that the leadership and this Senate and this House were informed in such a way with a very aggressive kind of consensus that was not shared when we had them before the Committee.

That's not been too long ago. And then, 30 days later, because of detainee information that's been so highlighted here, why, then we decided, well, you know, we just didn't have a consensus. Now, damn, that's got to quit. Now I know that you can't have every source and have a consensus threat analysis that's perfect. I'm not asking that.

But at the time, when you had the same people at same table, you know, one of my questions is, do you people know each other? And again it was information access. Now I feel very strongly about that. And I think it was a classic example of why you have to go back—the Vice Chairman calls it red teaming—and take a look at this, and say, well, what in the heck went wrong? Because we panicked, the entire Congress, not to mention Washington, DC., so on and so forth.

Thank God it didn't happen. You know, maybe I'm wrong. Maybe there was an element there that we missed. But it certainly was not present in regards to the presentation that we received.

Senator Wyden.

Senator WYDEN. Thank you, Mr. Chairman. As you know, I share your concerns about this whole question of how information is shared, and that's one of the reasons I raised the questions I did on the last round.

I'd like to go into another area, though, that goes to the heart of what I think the challenge is in America. I believe strongly in the proposition that our country has got to fight terrorism relentlessly and ferociously. And it's got to be done in a way that's consistent with protecting the privacy of law-abiding people, innocent people.

Now it's been 2 years since the Congress closed down the Operation Total Information Awareness program, but the Congress is still totally in the dark with respect to what kind of information your agencies collect on citizens and how it's used. And I want to be very specific and talk about data mining.

Data mining, by the way of shorthand, is essentially technology that your agencies use to sift through the records and information that involves millions and millions of American citizens. I can't find any rules on data mining anywhere.

And so what I'd like to ask each of you is, what do your agencies do with respect to data mining, A? B, are there any rules at all? And, C, how are the rules enforced? Because I've spent a lot of time on this. And I cannot find any rules at all on data mining.

So maybe if we just go right down the row.

Admiral Loy.

Admiral LOY. Sir, you and I have spoken about this a lot, as it's been perhaps 18 months or 2 years ago associated with, at that point, the Computer Assisted Passenger Pre-Screening second program, then known as CAPPS II. As you know, I have worked very, very hard to work with the privacy community and with many others attendant to recognizing what then became a list of eight absolutes that the GAO report initiated for CAPPS II and is now ten items that the Congress put in the appropriations bill last year for this department, attendant to, "You're not going any further with CAPPS II—and it's now Secure Flight, the new program—until all ten of those concerns that we have as a Congress are taken care of."

We have very diligently gone to great lengths to explore each and every one of the eight, each and every one of the now ten, and are right on the cusp, I believe, of satisfying the Congress and satisfying GAO that it is the right thing for us to press on with that particular program, because it has come to represent three things.

Senator WYDEN. Admiral, are you saying that that's the only program that involves data mining at your agency? I appreciate what you've tried to do, and you've certainly been a straightshooter on it.

What I'm concerned about is whether there are any rules with respect to data mining generally. I do know what happens when Congress picks up on one thing or another and suddenly the travel records get out on somebody. You all work with us. We try to get something to deal with that specific problem. But I don't see any rules with respect to data mining generally. And that's what troubles me.

Admiral LOY. I do not have a management directive in force, if you will, in the Department that I'm aware of covering data mining.

Senator WYDEN. Are there plans to do that?

Admiral LOY. I'll be happy to take that on and work with you, sir.

Senator WYDEN. All right. Let me just go right down the row. We've established at least one agency, other than the computer-assisted travel records, doesn't have it.

Yours, sir?

Admiral JACOBY. Senator, we have very clear, definitive restrictions on what the Department of Defense can do with respect to having any information having to do with U.S. persons in our files. And those are very conservative interpretations and they are regularly inspected by inspectors general at all levels inside the departments.

When we apply data mining tools against the information that we have available, there's no U.S. person's data in there to begin with. So it's a bit different situation than maybe some of the other departments.

Senator WYDEN. So you get no data, for example, from non-governmental sources, sir?

Admiral JACOBY. We are not permitted to maintain information on U.S. persons, sir.

Senator WYDEN. OK.

Director Goss.

Director GOSS. As you know, the National Foreign Intelligence Program was specifically set up to make sure that Americans do not spy on Americans and our work is done overseas. And I think that the proposition you have given us is one that, when I left Congress, was still red-hot after a couple of years of debate, which I think will go on. And that is the crossroads between privacy and protection.

As far as I know, our agency is not a relevant agency to answer your question, because we don't do data mining on U.S. persons unless it's under some safeguarded procedure which is properly notified and so forth.

Senator WYDEN. That's what I'm curious about. I know there are areas where you do it, and I'm wanting to know what the safeguards are. You're saying you don't do——

Director GOSS. The safeguards are notification of this Committee, sir.

Senator WYDEN. Director Mueller.

Director MUELLER. Well, we have one entity in the counterterrorism area called the Foreign Terrorist Tracking Task Force that, accomplishes certain data—I wouldn't call it data mining, but requesting from sources outside the Bureau information relating to possible locations of terrorists in the United States. And that has been briefed to Congress on a number of occasions. It's transparent. We're happy to have you come over and brief on it.

Senator WYDEN. That's the only set of rules you have with respect to data mining?

Director MUELLER. Well, it's not the only set of rules in terms of data mining. You're definition of data mining——

Senator WYDEN. That's what I'm asking.

Director MUELLER. We have information that's brought into the Bureau.

Senator WYDEN. Right.

Director MUELLER. When information is brought into the Bureau, it's brought in on predication. We have some reason to bring the data in. It may be telephone numbers. It may be addresses of potential terrorists. Now, we data mine that data. But it's data that we have a basis for bringing into our databases, whether it comes from our cases or from the collection of intelligence that is based on adequate predication.

Senator WYDEN. The reason I'm asking the question is that there are a lot of people in this country who believe that a lot of this information, you know, data mining, takes place without predication. And that's why I'm trying to figure out what the rules are. And I'm going to let Ms. Rodley answer the question. Then I'm going to ask something of all of you, and let my colleagues wrap up.

Ms. RODLEY. Senator Wyden, as you know, the State Department is not an intelligence collection agency. To my knowledge, the only information that we collect and maintain on American citizens is passport information. And passport information is held very closely and has a very strict set of rules regarding its use. I believe, but I will confirm to you later, that that's restricted to use for notifying next-of-kin when an American citizen is injured or dies abroad and cooperation with law enforcement.

Senator WYDEN. Thank you.

What I'd like from each of you is to confirm in writing what policies exist with respect to the sifting of information on Americans. And I would like it also to include how information is used, if it's used at all—and I understood that the Pentagon they had nothing—how it's used when it comes from non-governmental agencies where there, I think, is really the Wild West.

I mean, it's one thing if it comes from a Government agency. It's quite another if it comes from a non-government body. And having spent a fair amount of time digging into this area, I can't find what the ground rules are for data mining.

Can I ask, then, that each one of you will get us the ground rules you use for data mining within the next 30 days?

Director GOSS. Absolutely, sir.

Senator WYDEN. Thank you, Mr. Chairman.

Chairman ROBERTS. We thank you for your patience, your perseverance and your commitment to our country. Thank you very much.

This hearing is adjourned.
[Whereupon, at 1:17 p.m., the hearing adjourned.]

○