

House Permanent Select Committee on Intelligence

Chairman Mike Rogers Opening Statement

Worldwide Threat Hearing

February 10, 2011

***Remarks as Prepared**

Good morning. The Committee will come to order.

I welcome Director Clapper and our other witnesses this morning. You are very busy people, and I appreciate you all taking the time today away from the important work back at your agencies to participate in today's hearing.

Please pass along our thanks to the men and women in your agencies for their commitment and dedication in the defense of our nation.

I also welcome Dutch Ruppertsberger as the Committee's new Ranking Member. He is a solid leader, and his dedication and talent will serve the Committee and country well. Dutch is also a friend, and I look forward to working with him to foster the strong bipartisan energy we need to lead this Committee in our oversight responsibilities and to keep America safe. And, of course, it never hurts to have a former prosecutor on the job.

I'm looking forward to the discussion of threats in the witnesses' statements, and the questions and answers that follow. Before we get to that, I want to talk a moment about where I would like to take the Committee in this new Congress.

Reasserting Oversight:

It is a profound honor, and a tremendous responsibility, to assume the role of HPSCI Chairman at this important juncture in our nation's history.

The U.S. Intelligence Community is vital to defending our nation from the many threats we face. I have no doubt that the hard work of our intelligence professionals is one of the primary reasons there has not been a successful major attack on the homeland since 9/11 despite numerous failed and disrupted plots, and al Qaeda's unrelenting efforts to attack us.

Our job here in Congress is to make sure our intelligence agencies have the tools and authorities they need for their important mission, and that we never stop working to improve the Intelligence Community's effectiveness.

That begins with reasserting the House Intelligence Committee as the force for serious bipartisan oversight it was intended to be when it was established in 1977. I plan to do my part to restore that tradition, and I'm going to need the help of every member of this Committee to get that done.

I intend to restore a critical function of the committee - passing a meaningful annual intelligence authorization bill. We are already working on an FY11 bill, to be quickly followed by one for FY12.

The 9/11 Commission recommended that the Congressional authorization and appropriation committees work more closely on intelligence matters. I'm happy to announce that the House Intelligence Committee voted unanimously yesterday rules to allow Members of the appropriations committee to participate in our hearings and briefings.

I'm looking forward to working closely with my colleagues on the Appropriations Committee to eliminate the daylight that existed between our intelligence bills in the past.

10th Anniversary of 9/11

The 9/11 attacks transformed our country and the way we view national security. Since that day, the many threats we face have continued to evolve and grow in complexity. As these threats evolve, our response needs to keep pace.

In the face of this rapidly changing environment, and with the 10th Anniversary of 9/11 attacks coming up this year, it is an appropriate time for this Committee to take stock of the last ten years and examine whether the tools and institutions we've created are working, and whether they are positioned to face the threats of the future.

Tools: Congress has made comprehensive, historic changes since 9/11 to update the laws that authorize and govern our intelligence activities. We need to keep working to ensure that those laws keep pace with the new threats and rapid changes in technology.

- Critical provisions of the **Foreign Intelligence Surveillance Act (FISA)** expire at the end of this month. We need to rapidly reauthorize these provisions while examining other laws, like the **Communications Assistance for Law Enforcement Act (CALEA)**, that are in need of modernization. FISA has been vital to protecting our nation, and we need to work toward making its tools permanent parts of our arsenal.

- We must also reinforce **legal authorities concerning detainees** – one of our best intelligence sources in the war on terrorism. We need a system for intelligence exploitation and long-term detention that is flexible and can endure changing circumstances and court challenges, no matter where a detainee is picked up in the world. Executive Orders and other band-aids are not good enough; this problem requires a legislative solution.
- **Recidivism among released GTMO detainees** has also reached an alarming rate -- 25%, and those are just the ones we know about. We need to take a hard look at the detainee transfer and release process.

Institutions: We have had a good debate over the last decade about the institutions we put in place after 9/11 to prevent another attack, particularly the Office of the Director of National Intelligence, the National Counter-Terrorism Center, and transforming the FBI to be more of an intelligence-driven organization.

- We need to move beyond the debate about whether the DNI's staff is too large – this misses a more important point. The size of the DNI's staff can almost certainly shrink, but the real issue is what are we asking the DNI to do – missions should drive the size of the staff, not an arbitrary number. Director Clapper, you have some good ideas about **how to better organize ODNI**, and I want to help you succeed.
- The **FBI is a unique and vital institution**, straddling the foreign and domestic threats to our security. As a former FBI agent, I am especially interested in the efforts of the FBI to build an intelligence service within a law enforcement agency, and better adapt the Bureau's culture and practices to the rapidly evolving threat of terrorism.
- Certainly the FBI has made progress in this regard since 9/11, and has become much more intelligence-driven. But as the Fort Hood tragedy illustrates, we must accelerate the pace of this progress.
- Al Qaida has increased the use of westerners and Americans to penetrate our defenses. As we saw with the Fort Hood tragedy, this threat is further complicated by acts of violence by homegrown and "self-radicalized" American militants. We depend on the FBI's unique role to address these complex and growing threats.

Budget

Our nation has invested heavily in our intelligence capabilities since 9/11, and the **intelligence budget has grown exponentially** in that time. There is no doubt in my mind, however, that we got an outstanding return on that investment in terms of real improvement to our security.

History is littered, however, with examples of the consequences of nations that lived beyond their means for too long. Not surprisingly, the American people have become justifiably concerned about our budget deficit.

We must **seek greater efficiencies in your existing budgets to either fund new or expanded intelligence programs** or return those savings to the American people.

I understand that achieving **significant efficiencies in your intelligence budgets will require some hard choices** and I look forward to having a good discussion with you all about the pros and cons of different approaches to getting there in the coming months and years.

- For example, I urge the Intelligence Community to remain open-minded about alternative satellite architectures that could potentially meet current requirements at a much lower cost to the tax-payer. I haven't made up my mind yet, but I'm studying my options carefully, and so should you.

While further budget growth is unlikely in this difficult fiscal environment, I will hold the line against any cuts that endanger our key intelligence capabilities. **Intelligence is not a luxury** - I want to **avoid the mistakes of the 1990's when we cut too deep** in important areas of the post-Cold War intelligence budgets.

Making sure that our troops have the best intelligence support possible is also one of my highest priorities, and I intend to **focus more in the coming years on the Military Intelligence Program (MIP) budget**.

- The HPSCI is the only authorization committee with jurisdiction over both the National Intelligence Program (NIP) and MIP budgets, and is in a unique position to ensure that our civilian and military intelligence efforts are fully integrated and coordinated.

Mr. Ferguson, I understand that a reprogramming of MIP funds that is currently before Congress was not provided to this Committee. As I am sure you are aware, under House rules we have concurrent jurisdiction with the Armed Services Committee over the MIP budget.

- I'm sure this is a misunderstanding and that it was never the Department of Defense's intention to not keep the House Intelligence Committee fully and currently informed of these matters as the law requires.
- I understand that you have requested that Congress respond to this request by Friday. I would appreciate your assistance in quickly getting this problem resolved so that there are not any unnecessary delays to the reprogramming of these funds.

Cyber

As the **role of technology** in our lives becomes increasingly complicated and our technological dependence grows, the cyber threat from state and non-state actors grows at an even faster rate.

The creation of Cyber Command at Fort Meade was a step in the right direction to address the increasingly grave cyber threat, but we are **going to need some legislative changes to achieve the necessary unity of effort** across the larger U.S. government, as well as to bring more unity of effort across the private sector. We have great talent in some corners of the U.S. government when it comes to cyber-defense, we just don't have the right policies and legal authorities.

The Speaker has asked Congressman Mac Thornberry of this Committee to lead the efforts of the House on this important issue. He will have the full support of the House Intelligence Committee in the development of cyber-security legislation.

- As we move forward with this legislation, I believe we need to have a good debate over where to draw the boundaries of what the U.S government defends; and how we can help any critical infrastructure or industry players that are left outside that perimeter defend themselves.

Wikileaks

The **Wikileaks** fiasco should lead to an increased focus on our **information sharing** within the U.S. government. We missed critical opportunities to prevent the 9/11 attacks because of failures to share information between government agencies.

The Intelligence Community has made tremendous progress since 9/11 in improving information sharing, and we cannot allow the Wikileaks disaster to be an excuse to halt or reverse that progress. **We need to make sure we learn the right lessons from Wikileaks.**

- The right lesson is to redouble our efforts to promote information sharing while protecting security – what I like to call “**smart access.**” Smart access is an identity-based information security management system that improves our ability to detect and deter the few bad actors, and not unnecessarily punish responsible actors by denying them access to the sensitive information they need to get their work done.
- In response to the Wikileaks fiasco, the Intelligence Community and Defense Department have put together a good plan to implement smart access tools like auditing controls to detect the misuse of our sensitive data, similar to the systems credit card companies use to detect fraud.

These long overdue smart access fixes will not be cheap, but I believe they are well worth the price. This committee will monitor the implementation of these fixes and will work to identify any additional steps that are necessary to ensure that our sensitive data is secure.

Conclusion

I would like to thank the witnesses again for your participation in today's hearing.

You are running intelligence services, whose work is necessarily classified, inside the most open society in human history. The Congressional intelligence oversight committees are the connection between the arcane business of intelligence and the American people. Through strong and effective oversight, we are able to assure the American people that you are doing everything you can to keep us all safe, and in a manner consistent with American values.

Intelligence is an all too human business, and mistakes are inevitable. In fact, if you never fail, you're probably not doing what you need to be doing. What is important is that when a mistake happens, we talk in an open and forthright manner about what went wrong, and how to prevent it from happening again.

I look forward to working with you all to make sure that America has the best intelligence capabilities possible to face the dangerous world we live in. It is my hope that we can be partners, and not adversaries in this process.

Thank you, and I yield to the Ranking member for any statement he would like to make.

###