# Opening Statement: World Wide Threats
# February 4, 2014
# Ranking Member Ruppersberger

Thank you, Chairman Rogers.

First, I would like to acknowledge the leaders of our Intelligence Community, including:

- Director of National Intelligence, James Clapper

- CIA Director, John Brennan

- Director of the Defense Intelligence Agency, Lieutenant General Michael Flynn

- FBI Director, James Comey

- Matthew G. Olsen, Director of the National Counterterrorism Center

Thank you for being here today.

Throughout 2013, the Intelligence Community continued to provide policy makers with the vital information necessary to promote the values and interests of America, as well as to protect and defend it.

They did so amidst profound challenges, not only abroad, but at home, too. Be it in Syria or Boston, the Intelligence Community has worked tremendously hard. This past year, the IC has had to work amidst the worst leaks of classified information in our country's history.

Make no mistake: when we hand over our classified information, our adversaries and enemies adjust accordingly. We know this has already happened as a result of these leaks. Terrorist networks like Al-Qaeda and foreign countries are changing their tactics to avoid our detection. With this, the work of the Intelligence Community to respond and uncover threats becomes that much harder.

We must not forget that these authorities and capabilities are in place to keep our country and its citizens safe. While the intelligence community has followed the law—that is clear—it is apparent that the public has lost confidence in these programs.

I believe we must adopt important reforms to restore America's confidence in what the Intelligence Community does. We must increase transparency, strengthen oversight and improve safeguards to privacy and civil liberties.

I now want to look ahead to the challenges of 2014.

The threats we face continue to grow.

There is no greater example of this than the threats to America's cybersecurity. While the House passed the Cyber Intelligence Sharing and Protection Act (or, as we know it, CISPA) last year, CISPA has not yet become law, even though we worked very closely with the White House, the Intelligence Community, critical infrastructure companies, various industries across the technology spectrum, and privacy and civil liberties groups, to greatly improve the bill.

This means that the Government still cannot fully share cyber threat intelligence with the private sector, and the private sector cannot share cyber threat information with the government. In the meantime, countries and terrorists continue to attack our economic infrastructure, our trade secrets, and our critical infrastructure.

We hear about these attacks in the news everyday. Early last year, for example, our financial sector suffered a wide-scale network denial of service attack that proved difficult and very costly to mitigate. The retail giant, Target, is another recent example of our vulnerability to cyber-attacks.

We also have to do far more to expand our bench of cyber professionals and innovators, by investing in early education in science, technology, engineering and math (STEM). Our adversaries are making heavy investments in the education of their youth, and we must do the same.

Education is the keystone of security and prosperity in the 21st Century.

As far as collection priorities in this year, the Intelligence Community must remain vigilant on Iran. We must recognize that our consistent vigilance and our tough sanctions have brought us to a point where I believe important progress can be made on ending Iran's nuclear program.

I am hopeful, yet realistic, on where we are and where we can go: with sound intelligence, strong diplomacy, and robust defense, I am encouraged that more can be done to keep a nuclear weapon out of the hands of Iran.

In Syria, unfortunately, there is less cause for optimism. I applaud the agreement to remove Syria's chemical weapons; but I am increasingly troubled by the delays. We must keep our attention focused on completing this process, and doing so quickly.

At the same time, we must not lose sight of the horrendous humanitarian crisis that continues in Syria, and we must remain vigilant against the rise of Al-Qaeda and other extremists there. The area has become a magnet for terrorists, further destabilizing an already fragile region. We must ensure they do not make their way to America's shores or hurt our interests and allies overseas.

And violent extremists are not just a problem in Syria. In 2013, we saw AQAP, AQ's Yemeni faction, and the group's North African affiliate, AQIM, pose a very severe threat to the U.S.

In August, the threat forced the State Department to close 19 embassies across the Middle East and North Africa in response to an AQAP plot that was—thanks to your efforts—intercepted.

On the other hand, AQIM successfully conducted an attack against Western interests in Mali and Algeria, while Somalia-based terrorist group Al Shabaab committed a brutal attack in Kenya.

As for China, we continue to look with great concern on their cyber activities, their counter-space posture and on their recent moves in the East China Sea.

Beijing's so-called "Air Defense Identification Zone," which would require U.S. forces to identify themselves and their mission to Chinese forces as they fly near or over certain tiny islands, is a troubling power and land grab.

It is also an affront to international law. These moves increase the risk of misunderstanding and miscalculations between Washington and China, making the role of intelligence that much more important.

In Russia, our athletes, and athletes from around the world, will be convening in just a few short days to compete in the 2014 Winter Olympics. In the past month, we have seen some troubling terrorist activity, and we must keep up our guard.

In Afghanistan, 2014 marks the year in which combat operations end—but we know our vital national security interests there will not cease. We need to maintain our intelligence efforts there, even after the military withdraws.

Core Al Qaeda and the Taliban will continue to represent a threat; but we must not forget that Afghanistan is more than a front in the counterterrorism war. Afghanistan has broader strategic implications. It borders both Iran and Pakistan, and is close to both Russia and China.

This year, we must also continue to focus attention on space. We must continue to promote our commercial space industry, and relax those outdated regulations that are hampering our competitive advantage.

I cannot emphasize enough that US companies must also be allowed to compete in a free market. This competition will promote innovation in our space industry.

Finally, we need to rely on the Intelligence Community to look where others are not, to lift their gaze beyond the shiny objects of today. We need you to identify long term trends that cut across individual states or groups.

These trends, be they environmental, demographic, or technological, are the emerging fault lines of conflict. Early action can avoid long term pain.

And we need to do all of this, and everything we do, in ways that protect civil liberties. Liberty and security are not mutually exclusive. We can and must work to protect both, and we must remain ever-vigilant in this area.

I look forward to hearing from you on these challenges facing our country, how you plan to address them, and how you are going to work individually, and together, to do so.

And finally, before I close, I want to take a moment to appreciate the men and women of the Intelligence Community who are working to keep us safe 24 hours a day, 7 days a week.

Especially with the Government shutdown of last fall and the leaks, we heard a lot of negativity in 2013 directed towards federal employees generally, and our intelligence professionals specifically. This is unfounded and unjust.

These federal employees work nights, weekends, holidays, and in some of the most remote and dangerous locations to promote and defend the nation.

And they do so not for money, and not for fame—since they must often remain anonymous—but for love of country and dedication to its ideals.

Mr. Chairman, I yield back.

###

# Questions

1. **Cyber-security (to promote CISPA)**– Year after year we are witnessing the cyber threat slowly and steadily encircling us. As the capabilities to attack us grow and our vulnerabilities increase, we, however, largely stand by and watch. For every good—be it electronic health records that improve patient care and drive down health care costs, or the increasing amount of "smart" devices in our homes, offices and cars—we need to realize that we become that much more vulnerable to cyber bad actors who have the proven means and desire to do us harm. We need to hear from you what you need from Congress to help keep us safe and why.

2. **Satellite defense/security** –In 2007, China conducted a destructive antisatellite test against its own satellite. The debris field was troubling enough to our satellites and our space missions—but these early activities reveal that countries are working on the ability to destroy our satellites, on which so much of our daily lives, and our military and intelligence capabilities, depend. Please describe the counterspace threat and what can we do to better protect ourselves. I am particularly interested in whether Chinese leadership fully realize the ramifications of disabling one of our satellite systems?

3. **Afghanistan** –We all know the strategic importance of Afghanistan to the counterterrorism effort, which does not go away just because our troops withdraw. But, I think we need to understand whether there are broader regional or strategic implications of failing to secure a suitable Bilateral Security Agreement there.