# Opening Statement
# Ranking Member Adam Schiff
# Worldwide Threat Assessment of the U.S. Intelligence Community
# February 25, 2016

Thank you Mr. Chairman. I want to join you in thanking our witnesses: Director Clapper, Director Brennan, Director Comey, Lt. General Stewart, Director Rasmussen and Deputy Director Ledgett. We are very grateful for your efforts and for those of the men and women of the Intelligence Community.

The threats we face today are incredibly diverse and incredibly daunting. From cyber to terrorism, Russian aggression to North Korean nuclear belligerence. From threats to space to threats from below the sea. We are living in a dangerous world.

Because of technology, some of these threats are new. The Internet of Things, for example, presents unique vulnerabilities to the most advanced nations, like us, as does the rise of Artificial Intelligence.

Other threats are more traditional—but still potentially devastating. North Korea's January nuclear test and its recent space launch, Russia's interventions in Ukraine, Syria, and its threat to the Baltic States, China's activity in the South China Sea, and regional power struggles in the Middle East are a reminder that traditional, state-based threats have not receded. Far from it, they are getting worse.

Still other threats are shifting. Even as coalition bombing has halted the group's expansion in Iraq and Syria, for example, ISIS has thrown off spores into places like Libya, and has sought to incite attacks in Europe—as we saw in Paris—and to inspire attacks here in the United States, as we saw in San Bernardino.

Many of these threats are also interrelated. ISIS's virulence is compounded by its use of technology, particularly social media and encrypted communications. Russia's terrestrial ambitions and China's naval designs are supported by a desire to counter the U.S.'s predominance in space. And our greatest cyber capabilities are also our gravest vulnerabilities.

To navigate through all these treacherous shoals, we look to the IC to sound the alarms—as you are doing today—and to find and enable solutions.

After the Senate's version of this hearing earlier this month, many were saying that the world was going to hell in a handbasket and I can certainly understand why – given the myriad of challenges we face. But I want to emphasize here that we are highlighting the threats so we can discuss how best to counter them. And we have faced and overcome far greater challenges in the past.

To that end, we have begun receiving and reviewing your budget submissions. We look forward to many more sessions with you to make sure you have what you need to protect against these threats, and to do so in a way that is lawful, protective of privacy and civil liberties, cost effective and in keeping with the highest of American values.

Some solutions – particularly when it comes to the debate surrounding encryption – are not going to come easily. That simple fact is exemplified by this month's case involving Apple.

One thing, however, is clear – the court's ruling, even if narrowly tailored to the particular facts of this case, will have ripple effects that will significantly impact the law enforcement community, the intelligence community, the business community and all of us individually.

This case, and others like it, implicate policy questions that can't be decided by courts alone. Congress—through inclusive discussions with tech companies, interest groups, the public, the global community, law enforcement and the intelligence community, and the White House—must carefully weigh the competing policy considerations and arrive at sensible solutions.

As a first step, we need facts. That's why several months ago Chairman Nunes and I asked the National Academy of Science for a report on this issue, which will be completed this year. That's also why I support a legislative commission on encryption and the President's broader cybersecurity commission. A hard look at the most commonly advanced claims—on all sides of this encryption debate—would move us further from abstractions and towards solutions.

As a second step, we need to honestly acknowledge the complexity, and not engage in absolutes. As this Committee has shown with its leadership on surveillance reform and cyber information sharing legislation – privacy and liberty can and must co-exist.

There is no doubt that terrorists are exploiting cheap and widely available encryption technology to do us harm, and they'll continue to do so. At the same time, there is no doubt that our cybersecurity and our privacy are under relentless attack from nation state and criminal hackers, and greater encryption provides a key defense.

We can all agree that law enforcement and the intelligence community have an obligation to investigate crimes and prevent harm to Americans. Similarly, there is no doubt that American companies have obligations to their shareholders to maximize profits in an increasingly competitive global world, and to their customers to safeguard privacy.

Our job in Congress is to reconcile these legitimate obligations and priorities. It is our job to draw the lines. I am not advocating for a broad mandate on decryption, but nor do I favor a world where law enforcement is completely shut out of illicit communications when they have a court-approved warrant.

What I am advocating is for a cooperative, fact-based approach to solving this very real problem. Congress can impose a solution if it must, but it would be far better for us to arrive at a resolution through a negotiation with all the stakeholders that sets the standard for best practices and one that we can live with at home and champion around the world.

Yes, we are living in a dangerous world, as well as a complex world—make no mistake about it—but it is also a world of great opportunity.

Some of the challenges we have today, like that presented by encryption, are borne of the incredible talent, creativity and innovation of American businesses that are solving problems every day. We also have the best Intelligence Community in the world working tirelessly to make sure these advances are not used to propagate hate, violence, and terror through channels that are beyond reach.

The challenges and the answer to these challenges lies in finding solutions together.

Thank you Mr. Chairman, and I yield back.