

Opening statement

Chairman Nunes: The Committee will come to order. Today, the Committee will examine World Wide Threats. I would like to welcome our witnesses: Director of National Intelligence James Clapper, Director of the Central Intelligence Agency John Brennan, Director of the Federal Bureau of Investigation James Comey, Deputy Director of the National Security Agency Richard Ledgett, Director of the Defense Intelligence Agency Lieutenant General Vincent Stewart, and Director of the National Counterterrorism Center Nicholas Rasmussen. Thank you all for being here today.

I recognize the challenges associated with discussing sensitive national security issues in public, but I hope you agree that this open forum is critical to help explain to the American people the serious threats that we face, and also to highlight the efforts of the brave men and women of the Intelligence Community to keep us safe. I speak for the entire committee when I say thank you for your service, sacrifice, and dedication. Director Clapper, as this is your last World Wide Threats hearing with this Committee, I'd like to specifically thank you for 55 years of service to this great nation.

Director Clapper, I recall from last year's testimony that you were concerned about a vast array of threats. Remarkably, the number seems to have grown since then. Generally, I share your assessment of the current threat environment. The truth is, the United States today faces the highest threat level since the 9/11 attacks. The American people don't need a security clearance to understand the threats now facing the Western world; they only need to read the headlines out of Paris, Brussels, San Bernardino, and Boston. Al-Qa'ida, ISIS, and other terror groups are expanding rapidly, with more access to safe havens, recruits, and resources than ever before. Without U.S. leadership, this trend will continue.

We have discussed Syria and Iraq with you at length in closed and open sessions. I believe the U.S. response to those conflicts is among the most mismanaged foreign policy blunders in recent history. After consistently failing to block ISIS's expansion, we have to accept a new reality; ISIS is now in dozens of countries and has repeatedly demonstrated the ability to reach our homeland. Instead of focusing on ISIS as if it were confined to Iraq and Syria, we urgently need an aggressive, comprehensive, anti-terror strategy that stretches from Morocco to Southeast Asia.

At the same time, our adversaries are becoming more diverse. Throughout the next decade, the U.S. must be prepared to check Chinese ambition in Asia, counter a resurgent Russia, defend against cyber threats, and manage delicate geopolitical forces in the Middle East, including the growing schism between Sunni and Shia Muslims. How does the President respond to these enormous challenges? His hallmark policy has been to strike a nuclear deal with Iran that greatly relieves pressure on the Iranian regime – the world's biggest state sponsor of terrorism. He also failed to prevent Russia from propping up Syrian dictator Bashar Assad – a man whom the President himself has insisted must surrender power. Meanwhile, some of our closest allies in fighting terrorism – the Kurds, the Israelis, and the Egyptians – often find their concerns downplayed or dismissed within this administration. Our partners around the world want to work with us, but they can't rally behind American leadership if they don't understand what our foreign policy is trying to accomplish.

Although many Members of this committee disagree with the President's policies, the committee will continue to provide the Intelligence Community with the resources it needs to protect the nation, with particular emphasis this year on preserving capabilities for the next President. Because the Intelligence Community is being stretched thin and is overwhelmed by a complex threat matrix, we must prioritize investments throughout the entire Intelligence Community.

Our committee's mission is clear: we help the Intelligence Community to protect the American people by providing oversight, direction, and resources to enable effective, efficient, and constitutional intelligence activities. Additionally, amid the growing threats we face, it is critically important that we ensure that the Intelligence Community act as a careful steward of taxpayer dollars.

Over the next several years, our committee will focus on making progress in the following key areas:

1. Encouraging efficient investment in areas such as space in which complex program and capability requirements routinely drive up costs, and adopting new technology, including data analytics, encryption, and technical training, specifically in community-wide projects like cloud computing, data security, and tool management.
2. Reassessing the effectiveness of the community's human intelligence enterprise and synchronizing community-wide resources, especially at a time when several Intelligence Community agencies are implementing reorganization plans. This particularly applies to the recruitment and training of the next generation of collectors, cyber experts, and analysts to operate in nontraditional areas and deliver intelligence on hard-to-reach targets.
3. Producing objective and unbiased intelligence analysis, particularly in the Department of Defense, where there is a multi-committee effort to determine whether there are systemic problems across the intelligence enterprise in CENTCOM or any other pertinent intelligence organizations. In this context, it is vital that this committee protect and seriously consider the testimony of the many whistleblowers who provide information to us.
4. Improving the efficiency of intelligence support to the Combatant Commands, including efforts to curb facilities and personnel costs. It's alarming that this committee

identified up to \$50 million in annual savings for the Defense Intelligence Agency and more than \$300 million in new, unneeded construction disguised as base consolidation. In total, this was \$1.5 billion in savings for one project.

The response we've received from the administration can only be described as delay, denial, and deception. This has led the Chairman of the Armed Services Committee, the Chairman of the Appropriations Committee, and me to ask the Government Accountability Office to conduct a full investigation. Furthermore, whistleblowers have provided this committee with documentation showing that the Department of Defense has provided false information to Congress. This committee will now conduct another round of interviews and will turn over our findings to the House Committee on Oversight and Government Reform, which already has an ongoing investigation into the matter, and to the Department of Defense Inspector General.

Finally, we've asked for data on all intelligence personnel and major support contracts at the Combatant Commands. This request was made in December, so it should be readily available. Informants have made the committee aware that basing decisions are being determined by the locations where small groups of individuals want to live. This includes both Department of Defense civilians and contractors. This brings into question hundreds of millions of dollars of contracts that are being awarded annually.

5. Mitigating cyber threats and improving cyber defense in light of the rapid pace of technological change. To address these problems, this committee helped pass the Cybersecurity Act of 2015, while the Director of National Intelligence is establishing the Cyber Threat Intelligence Information Center. We need to ensure that the new law is implemented properly and that the new center operates effectively. Additionally, the latest challenges the government has met in gaining access to an iPhone used by one of the San

Bernardino terrorists is emblematic of the growing problem posed by encryption. Finally, we need to educate Members of Congress on the importance of reauthorizing section 702 of the Foreign Intelligence Surveillance Act.

I look forward to hearing what the witnesses have to contribute on these five areas. And with that, I would like to recognize the Ranking Member for any comments he would like to make.

Chairman questions:

- Director Clapper and Director Stewart, the Committee recently received ODNI survey results indicating that over 40% of analysts at CENTCOM feel there are problems with analytic integrity and CENTCOM processes. Since we can't afford to wait eighteen months for an Inspector General report, what are you doing to rectify these problems?
- Director Comey, can you briefly touch on the encryption debate, with respect to the San Bernardino shooter's iPhone? What exactly are you asking Apple to do? How does this differ from the other times you have asked Apple to help you lawfully obtain communications? Director Clapper, what are your views on the encryption issue?