**Privacy and Civil Liberties Oversight Board**
**Public Forum – February 8, 2019**
**Statement of Alex Joel**
**Chief, ODNI Office of Civil Liberties, Privacy, and Transparency**

**Introduction.**

Thank you for inviting me to speak at the Board's Public Forum.

My colleagues in the Intelligence Community and I are delighted that the Board once again has a quorum.

We strongly believe in the importance of the Board's mission, and welcome the Board's independent and rigorous oversight, as well as its advice.

I've been in this job since stand up of the ODNI in 2005. I've therefore had the privilege of working with the Board beginning with its first iteration, when it was part of the Executive Office of the President, and then with its second iteration as a stand-alone, independent agency. I am delighted to have this opportunity to work with all of you, and look forward to also working with the two remaining members once they are confirmed.

**Terrorist Threats.**

The Board's mandate is to provide advice and oversight with respect to the government's efforts to keep the nation safe from terrorism. Because it is important to understand the broader context in which our counterterrorism programs operate, I wanted to take a few minutes to describe the current terrorist threat environment.

In that regard, as you know, the National Counterterrorism Center has been providing detailed, classified threat briefings to Board, and looks forward to continuing those briefings going forward.

At the outset, note that the IC's mission is to focus on national security, and to provide the best FOREIGN intelligence we can. That means that for terrorism, we focus on international terrorism, including how foreign terrorist organizations reach inside the United States. There are, of course, very significant wholly domestic threats, which are the focus of other government organizations.

With that in mind… Director Coats recently appeared before Congress, along with other IC leaders, to provide the annual worldwide threat assessment. That assessment covered a range of threats, not just terrorism.

As Director Coats said, the composition of the current threats we face is a toxic mix of strategic competitors, regional powers, weak or failed states, and non-state actors, all using a variety of

tools in overt and subtle ways to achieve their goals. He pointed out that the scale and scope of the various threats facing the US and our immediate interests worldwide is likely to further intensify this year.

Regarding terrorism, Director Coats said that it remains a persistent threat and in some ways is positioned to increase in 2019. The conflicts in Iraq and Syria have generated a large pool of skilled and battle-hardened fighters who remain dispersed throughout the region. While ISIS is nearing territorial defeat in Iraq and Syria, the group has returned to its guerilla-warfare roots, while continuing to plan attacks, and direct its supporters worldwide. ISIS is intent on resurging and still commands thousands of fighter in Iraq and Syria.

ISIS and al-Qa'ida affiliated groups continue to try to motivate U.S.-based supporters to carry out acts of violence in the U.S., to further ISIS and al-Qa'ida goals.

Note that although there continue to be attacks in Europe and the United States, most terrorist attacks take place in countries in the Middle East, Africa, and Asia, and most victims are residents of those countries. The IC works closely with partners in those countries as part of an ongoing collaborative effort to combat terrorism worldwide.

The IC has also warned that violent ethno-supremacist and ultranationalist groups in Europe will employ violent tactics in pursuit of their aims. In the past two years, individuals with ties to violent ethno-supremacist groups in France, Sweden, and the United Kingdom have either carried out attacks on minorities and politicians or had their plots disrupted by authorities.

In terms of newer technologies, the IC has warned that terrorists could obtain and disclose compromising or personally identifiable information through cyber operations, and they may use such disclosures to coerce, extort, or to inspire and enable physical attacks against their victims*.*

That's a brief snapshot of some of the threats that the IC's counterterrorism programs and activities are designed to address. NCTC stands ready to provide more detailed information to the Board, including classified information, as part of its regular threat briefings.

**National Intelligence Strategy**

Another part of the strategic context for our programs is the recently issued National Intelligence Strategy, or NIS. This fourth iteration of the NIS establishes seven "mission objectives" and seven "enterprise objectives." The mission objectives broadly describe the activities and outcomes necessary for the IC to deliver timely, insightful, objective, and relevant intelligence. The "enterprise objectives" provide the foundation for integrated, effective, and efficient management of mission capabilities and business functions.

There is a standalone mission objective for Counterterrorism – Mission Objective 5 – a version of which, not surprisingly, has been in all iterations of the NIS. That objective states that the IC

will identify, understand, monitor and disrupt state and non-state actors engaged in terrorism and related activities, to defeat threats to the US, our people, interests, and partners.

The IC has been aggressively pursuing counterterrorism for many years, and intends to continue to do so. We stand ready to brief the Board on those programs and activities as part of the Board's oversight function, and to seek advice as new programs are contemplated.

Just as significantly, for the first time, there is a standalone enterprise objective in the NIS – Enterprise Objective 7. It states that the IC will safeguard privacy and civil liberties and practice appropriate transparency to enhance accountability and public trust in all we do.

There are three sub-objectives. The first looks inward, to incorporate privacy and civil liberties requirements into IC policy and programs. The second looks to our oversight entities and our partners. We need to make sure that the Board and other oversight bodies have the information needed to carry out rigorous oversight.

These first two sub-objectives reflect the traditional pillars of our framework – rules to protect civil liberties and privacy, and oversight to ensure we follow those rules. Traditionally, these vital processes have taken place in secure environments so that the full range of relevant information can be made available to oversight bodies.

This "secret" oversight is essential to a democracy. It ensures that those holding us accountable have full access to the information they need to perform their functions.

This framework of rules and oversight is necessary, but it is not, on its own, sufficient to earn and retain public trust.

That's where our third sub-objective comes in. If the first looks inside the IC, and the second looks to our oversight bodies and our partners, the third looks outward, toward the public, and calls on us to practice and promote public transparency.

**Transparency.**

The public must be able to understand who we are, what we do, what our rules are, and how we ensure compliance with those rules. At the same time, we must continue to protect sources and methods.

A few years ago, we issued the Principles of Intelligence Transparency for the IC. These are high-level principles that give us guidance and direction. They are included in the NIS.

The IC followed up on those principles by publishing an implementation plan, forming an Intelligence Transparency Council, and taking a range of concrete measures to live up to those principles. The IC established IC on the Record on Tumblr as a platform for publishing an extraordinary volume of formerly classified information documenting how we use key national security authorities, such as Section 702 of FISA.

The IC also prepared and published key reports, such as semiannual assessments of compliance under Section 702, and the annual statistical transparency report, which publishes a range of statistics on how the IC uses important national security authorities.

We proactively published the first two of those reports, after which Congress codified that report into law. When we proactively included additional statistics not previously required by Congress, it again codified those statistics into the annual reporting requirement.

In addition, we launched intelligence.gov as a digital front door to the IC. It features rich multimedia content and innovative approaches to conveying information. It also serves as a platform to host major repositories of intelligence documents, such as Bin Laden's Bookshelf, and the recently released documents on the Tet Offensive.

In addition, we've taken all documents posed on IC on the Record, and made them full-text searchable through a search feature on Intelligence.gov.

In March of last year, DNI Coats reissued our core Intelligence Community Directive (or ICD) – ICD 107. It was first issued in 2012 and focused on civil liberties and privacy. Under Director Coats, it's been revised so that it now includes transparency as well.

And now, transparency is part of the IC-wide NIS, setting strategic direction for the entire community. So we see the rapid evolution of transparency in the IC, from high-level principles, to concrete action, to mandatory policy, and now to forming an integral part of our strategy as a community for the next five years.

**Culture.**

Our commitment to civil liberties, privacy, and transparency is reflected in other ways, and has become part of the culture within the IC.

For example, the Principles of Professional Ethics, first issued in 2012, call on us to selflessly serve the American people, to seek and speak the truth, to respect privacy and civil liberties, to demonstrate integrity in our conduct, to be accountable, to seek continuous improvement, and to embrace the diversity of our nation.

Those principles are included in the NIS. We hand out badge buddies with those principles to incoming officers as they enter on duty, and to everyone on Constitution Day. At ODNI, on every Constitution Day, we retake our oath to support and defend the Constitution, and other IC elements hold similar events to reaffirm their oaths.

My counterparts across the IC also provide training on comprehensive rules that are in place to protect civil liberties and privacy, in order to further reinforce that culture.

In addition, one of the things we seek to do is to provide a safe space for our work force to raise concerns.

To that end, I have held many "Plain Talk" sessions with the workforce, both in person and online, where anyone can ask me any question related to civil liberties, privacy, and transparency.

We have also held a series of panels, in agency and interagency forums, to make sure people understand the various channels available to raise concerns.

The IC's IG community has stepped up its own training and awareness programs, which we strongly support. They have a strong presence on both public and internal websites providing information on how to make a complaint, and they rigorously investigate retaliation claims and enforce whistleblower protections.

**Looking Ahead.**

As I think you can tell, I feel we have accomplished a great deal, and I am proud of those accomplishments. But there is a more work that lies ahead. We welcome the Board's advice and oversight in that regard.

Looking ahead, I'll mention a few items where I think the Board might take an interest.

**ASTR.** The sixth annual statistical transparency report is coming up. These reports are important, and very challenging to prepare. We stand ready to brief the Board on those reports, including the classified information that supports them, and discuss what those reports convey about our use of national security authorities.

**UFA.** Certain provisions of the USA FREEDOM Act are set to expire at the end of this year. We will be working on transparency to support the public debate on those provisions. In particular, there is one provision that authorizes the government to obtain call detail records on a targeted basis from telecommunications companies, with individualized court orders. We expect to spend quite a bit of time on that provision in the coming months.

**AI/ML.** The IC has publicly discussed its strong interest in artificial intelligence and machine learning to support the work of our intelligence analysts. We are keenly aware of the privacy and civil liberties concerns associated with the development and deployment of those technologies.

**Technological change.** More generally, technology is changing ever more rapidly, while law and policy changes much more slowly. New technological developments will present risks and opportunities. We would welcome the Board's insights as we address those developments, and in particular, how technology could be used to protect privacy and promote transparency.

**International.** On the international front, as you know, some of our friends overseas have expressed concerns about how the IC protects privacy. We have done a great deal of work to address those concerns. The Board's engagement in this area would be welcome.

**Transparency.** Finally, we will continue to look for ways to improve our current transparency practices, and to develop new ones. The IC faces growing transparency demands, both from our own pro-active efforts and from external mandates including ever-increasing FOIA litigation. We have limited resources, and much of this work requires in-depth involvement of the intelligence experts who are conducting the activities. Only with their expertise is it possible to conduct the painstaking reviews that are necessary to make information public.

Nonetheless, even with these constraints, we know there is more we can and should be doing, and we welcome the Board's expertise and insight as we continue to improve our transparency efforts.

**Conclusion.**

Again, thank you for this opportunity to speak. We look forward to continuing to support the Board's vital advisory and oversight functions.