OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
Public Affairs Office
LEADING INTELLIGENCE INTEGRATION

Remarks as delivered by
The Honorable James R. Clapper
Director of National Intelligence

AFCEA/INSA National Security and Intelligence Summit

Thursday, Sept 18, 2014
8:30 a.m.

Omni Shoreham Hotel, Washington DC

Thanks for that introduction, Mark [Lowenthal]. Mark is a gifted tap dancer. It was close, but we made it. It was about ten light cycles to get across the Ellington bridge. It's great to be introduced by Mark – a friend and colleague of many years.

This is truly remarkable, to see INSA and AFCEA co-hosting this summit. It's extra special for me, because I'm somewhat of an "INSA hipster." I was into INSA before it was cool. [laughter]

Actually, I was into INSA before it was *INSA*. In the late '90s, I was president of SASA for a year or two, and I tried to promote – a word you'll hear again from me – *integration* with AFCEA. For a lot of reasons, that was an idea whose time just hadn't come yet. Now, it has.

So good on INSA and AFCEA for doing this. I trust it isn't just a one-off. So, accordingly, I especially appreciate the chance to kick off this summit. It has real meaning for me, having been associated with AFCEA and INSA in a prior life.

In one sense, the timing couldn't be better. We just sent the 2014 National Intelligence Strategy to the print shop and we decided this summit would be a great place to roll it out. So here it is [holds up copy of NIS] in hard copy.

And, just to prove the government can coordinate with itself, this morning, my office is publishing the National Intelligence Strategy on our public website: "dni.gov" … along with a press release. We're also tweeting about the NIS and updating our Facebook page.

I think these actions show just how much our intell environment has changed, because back in 2009, when we published the previous NIS, there's no way you could have convinced me I'd be talking about rolling out the next one on Facebook and Twitter. [laughter] In 2009, I didn't know what Facebook at Twitter even were. Only kidding. So for lots of reasons, it was time to write a new one.

Before I talk about what's in it, I want to ask – and then answer a rhetorical question: Why bother? – as in – Why do we even bother to write strategies anymore? I think there are three reasons.

First, it is useful to capture what we want our community to look like and how we want it to act, those attributes of our enterprise that are relatively timeless, meaning they're good for about three or four years, which is a long time in the national security world.

The second reason is because it is another way to promote integration of the 17 Intelligence Community components. "Intelligence integration" has been my major theme for the past four years I've been DNI. I believe it's the reason my post and my office exist. It's what the 9/11 Commission advocated, and what IRTPA – the Intelligence Reform and Terrorism Prevention Act of 2004 – legislated.

And the third reason is to help focus our resources, including people, in an ever-constrained budget environment. As Mike Hayden aptly points out: The process of writing and coordinating a NIS is important itself. So for me, those are the three reasons why we should publish a National Intell Strategy.

So what's actually in it? I should start by acknowledging my two personal contributions: First: I cut the original draft in half. [applause and then laughter] Thanks. I figured if it was shorter, there would be a better chance that more people would actually read it.

My second contribution: I only signed an unclassified NIS. One of my big takeaways from the past 16 months is that we need to be more transparent. And, if we're going to profess transparency, we need to practice transparency, whenever we can. So, there's no "secret" version of the NIS. Our oversight committees, our partners, the public, and for that matter even our adversaries are all seeing the very same strategic direction I'm giving to the Intelligence Community.

Showing things to our adversaries, by the way, is the other side, the down-side of transparency. But again, as Mike points out, nobody else on the planet does that, except us.

First and foremost, the 2014 NIS opens with our seven Principles of Professional Ethics for the IC. I'm going to come back to those in a minute.

Then, it lays out the strategic environment we're operating in. By the way, I went to great lengths since I left the Pentagon to stop using Powerpoint. But here, today, I thought we would do a few.

That strategic environment includes the global environment; which is composed of the most diverse array of threats and challenges as I've seen in my 50-plus years in the intell business; it discusses how globalization of technology brings both benefits and challenges, and speaks to how competition for scarce resources – like food, water, and energy, and I might add disease – is growing in importance as an intelligence issue as that competition foments instability.

As time goes on, we'll be confronting issues I call "basics" resources – food, water, energy, and disease –more and more as an Intelligence Community.

The strategic environment also includes the recent factors that affect IC capabilities, what I've referred to as a "perfect storm" that's dogging and degrading our capabilities: The theft and leak of NSA and IC documents – and loss of collection as a result, the resulting damaged relationships with foreign and corporate partners, our conscious decisions to stop collecting on some specific targets, overlaid, with our increasingly constrained budget resources.

As I tell my friends on the Hill, "Whatever you think about intelligence, you'll have a lot less of it to complain about." [laughter]

The result of this perfect storm is that we, as a nation, are taking more risk. In many cases, we've chosen where we're taking risk – cutting specific programs, stopping specific collections, declassifying specific documents. All of those are good choices, as long as we recognize that we, as a nation, have to manage the attendant risks that we will incur when we take these actions. And all of that is clearly part of the strategic environment we work in.

By the way, the culmination of all the turbulence that has beset the Intelligence Community over the past year or so is a new set of imperatives, which has spawned a new approach to the practice of intelligence, which I'm going to roll out here. Let me try to describe this new approach.

We are expected to keep the nation safe and provide exquisite, high-fidelity, timely, accurate, anticipatory, and relevant intelligence; and do that in such a manner that there is no risk; and there is no embarrassment to anyone if what we're doing is publicly revealed; and there is no threat to anyone's revenue bottom line; and there isn't even a scintilla of jeopardy to anyone's civil liberties and privacy, whether U.S. persons or foreign persons. We call this new approach to intelligence: "immaculate collection." [laughter]

Sorry, I couldn't resist. And by the way, we have to conduct "immaculate collection" on the cheap too.

Okay, back to what's in the NIS. After "Strategic Environment," the 2014 National Intelligence Strategy lays out seven mission objectives.

Three of those refer to foundational intell missions that apply to every region and topic. Strategic Intelligence informs and enriches our national understanding of enduring national security issues. Anticipatory Intelligence detects, identifies, and warns of emerging issues. You'll not find anything about clairvoyance, which some expect of us. And, the third foundational Mission Objective is support to current operations.

The other four Mission Objectives identify the enduring topical missions we have to meet, the "counters": counterterrorism, counterproliferation of WMD, counterintelligence, and cyber intelligence. This NIS emphasizes that "cyber intelligence" is a lot more than just "cyber security."

To meet those seven Mission Objectives, we need to accomplish six enterprise objectives that address our capabilities. The third major section of the 2014 NIS discusses those.

The first two of the six enterprise objectives relate directly to my mantra of intell integration. First, integrated mission management means that, instead of having the intell silos collect what they can, and then we sort out the data and analyze it, instead, analytic activities identify intell gaps and provide guidance on what information they need collected. And counterintelligence elements work closely alongside to identify vulnerabilities.

CI is an area, by the way, where I've been spending a lot of time, as of late.

Second, integrated enterprise management means strategic coordination of IC business practices and resources. That's everything from facilities, logistics, budgeting, and major acquisitions, to continuous evaluation and adjudicating security clearances, to providing transparency and protecting civil liberties and privacy.

So the key point for both our mission and enterprise issues is that we're much better off managing them as – drum roll – an integrated enterprise.

Our other four enterprise objectives describe how we build a solid foundation of key capabilities. Information sharing and safeguarding is talking about IC ITE [the Intelligence Community information technology enterprise], which I think most of you have heard about.

We needed about two years to lay the foundation. Now we've started adoption of integrated IT systems. We have the common DTE desktops rolling out. We have a working government cloud. And the commercial cloud came online in July. It's an important thing, the next big thing for intelligence, and it's becoming real.

And making sure IC ITE sticks is one of the biggest reasons my principal deputy Stephanie O'Sullivan and I agreed to stick around for maybe another 122 weeks, or 855 days, but who's counting? [laughter]

The fourth objective, "innovation," covers everything from R&D to tradecraft, and even creative ways to work within a constrained budget.

"Our people" includes Workforce Planning, Diversity, and Inclusion. I'll come back to that.

And finally, the objective on "Our Partners" includes: Our foreign allies & friends, and their intell services; our military and federal partners; state, local, tribal, and territorial governments; and our private sector partners.

The fourth, and final, section of the 2014 NIS goes into how we're implementing the strategy, including my role in setting direction and the roles for the IC elements to execute mission.

So that's what's in our new National Intelligence Strategy: the strategic environment we're operating in; mission objectives for strategic and anticipatory intelligence, supporting current ops, cyber intelligence, counterterrorism, counterproliferation, and counterintelligence; enterprise objectives for integrated mission and enterprise management, info sharing and IC ITE, innovation, our people, and our partners; and finally, how we're going to implement the strategy to meet those objectives.

I'd like to take the rest of my time, before I get to questions, to talk about the one-page section at the opening of the NIS, which I briefly mentioned earlier. That's the "Principles of Professional Ethics for the IC." It had a long journey to make it into the NIS.

I had, for a while, wanted to articulate, in one place, the fundamental ethical principles that unite and distinguish us – something that would help forge a unified IC identity, which encompasses the personal, organizational and corporate standards of behavior expected of us as intelligence professionals.

So in February of 2012, I asked our civil liberties protection officer to prepare a professional "code" of ethics for intelligence professionals. Early on that year, we wrestled with the question of whether we should even *have* a code of professional ethics.

It's something typically reserved for strictly-defined professions, like attorneys and doctors. So we needed to decide if it was even *possible* to write an ethical code that would equally apply to collectors and analysts from every INT, managers, our research scientists and engineers, and people in every support role.

To answer that question, we tapped the considerable academic work on the subject of professional ethics, including some thoughtful work done at the National Intelligence University.

We assessed that "intelligence" qualifies as a profession, because we in the IC have unique access and training, so we're capable of reaching informed decisions when the general public can't, and that's true across the IC.

On top of that academic reasoning, I felt that a professional ethical code was necessary because we live in a classified world, where the details of even our *oversight* are secret, and so it is even more important for us to hold ourselves accountable.

So during the summer of 2012, a cross-community team drafted seven principles. We built a consensus across the IC. And in September of 2012, two years ago, we published the "Principles of Professional Ethics for the Intelligence Community."

Unfortunately, September 2012 was also the start of a fairly turbulent year that included terrorists attacking Benghazi, nearly leaping off the fiscal cliff, actually falling into sequestration, suffering through the Boston Marathon bombing, enduring the press leaks, watching – with horror – the chemical weapons attacks by the Syrian government on its own people, and last October shutting down the government.

We got caught up in all those current events, and thus we fell short in our rollout and publicity of the Principles of Professional Ethics. But now, with the 2014 NIS, we were able to memorialize

the seven Ethical Principles into a more permanent publication that guides the entire IC. So I want to walk through them, and try to relate how they match my experiences.

The first Principle says, "We serve the American people, and understand that our mission requires selfless dedication to the security of our nation." I've been committed to that mission for 51 years, and I proudly include my six years with industry in that life-long commitment.

I've seen incredibly selfless acts, including men and women who have made the ultimate sacrifice, to include an intelligence officer recently.

But, that dedication also plays out in routine ways, like late on a Friday night, when an NSA team came to brief me on their work. I apologized that we couldn't find a more convenient time, one that didn't eat into their weekend. And the team leader told me, "Sir, our system collects on Middle-East targets around the clock during their work-week. Your schedule had openings during our work-week, but we weren't driving down here from Fort Meade to talk to you while our system was running." [laughter]

Something about young people keeping you humble. [laughter]

But also, as my incredible partner Stephanie O'Sullivan put it, "How can you not be motivated by that level of dedication?"

The second Principle gets to the heart of what our mission is. It says, "We seek the truth; speak truth to power; and obtain, analyze, and provide intelligence objectively."

Over the past two years, we in the IC have had way too many opportunities to give bad news to those in power, and we have not shied away from the truth. I know I certainly have had occasions to do that.

Some months ago, I told the President that he understands the IC and intelligence as a profession better than any modern-day predecessor. I just wish he'd gained that insight for better reasons.

The third Principle says, "We support and defend the Constitution, and comply with the laws of the United States."

Over the past 15 months, the theft and release of NSA documents has cost us sources and methods we won't get back. Yet to me, even more disturbing is that many Americans now question their IC's commitment to lawfulness, and to privacy and civil liberties.

We all, whether in uniforms or suits, take oaths to support and defend the Constitution, against all enemies, foreign and domestic. And, I would assert, we spend more time and energy focused on understanding the laws and directives that govern our work than any other sector of government. That's actually been true for a long time. And the facts of the past decade show that while we have made mistakes, to be clear, the IC never willfully violated the law.

And that, in turn, relates directly to our fourth Principle, which says, "We demonstrate integrity in our conduct, mindful that all our actions, whether public or not, should reflect positively on the IC at large."

This one is very personal for me, and became even more-so after I was accused of lying to Congress. It's been very disappointing to me, after half-a-century of service, to be questioned about my integrity because of a mistake in trying to answer, on the spot, a question about a specific classified program in a generalized unclassified setting.

But again, our mission is to seek truth and speak truth to power. That's what I've always done, and what I intend to keep on doing until I've got both feet in assisted living. [laughter] And hey, as President Truman said, "You want a friend in Washington? Get a dog." [laughter]

The fifth principle says, "We are responsible stewards of the public trust." Usually with stewardship, people talk about resources and money.

But when I think about stewardship, I first think about being a good steward of our most valuable asset, which is our people. Training and, especially, mentoring the people who will carry on the work of intell and intell integration in the next few decades has become an especially big deal to me, because, as my wife has made clear, I'm not going to be in this job more than another 122 weeks or 855 days. But who's counting?

I'd like to talk about that work of intell integration in terms of our sixth principle: "Excellence." I'm sure, many people here have heard the phrase, "silos of excellence." When you've heard or said that phrase, it probably wasn't meant in a positive context.

Usually, when I hear "silos of excellence," it's used sardonically to describe practices of stove-piping intelligence, and then is expanded to encompass everything that's ever been wrong with the IC.

But here's the catch: the excellence of the Intelligence Community really is bound up in those silos: the capabilities and tradecraft of each agency and component.

Integration does not mean turning the Intelligence Community into "one big, bland bowl of oatmeal." It does not mean making us the same. It means keeping the tradecraft in each silo of experts, and giving access to every silo to the men and women who produce intelligence.

Integration is about getting the best out of our diverse viewpoints and experiences by celebrating our differences and bringing them together. Those silos – those stovepipes – are the sources and keepers of some of the great strengths of our IC: our tradecraft.

And that leads me to our seventh and final IC Principle of Professional Ethics: "We embrace the diversity of our nation, promote diversity and inclusion in our workforce, and encourage diversity in our thinking."

In fact, embracing the diversity of our nation doesn't go far enough, when you think about it. We have to embrace the diversity of the world we're trying to understand. As Stephanie has said, you cannot look like me and operate on many of the streets of this world, and we need analysts whose understanding of unique global communities runs deeper than what they've read or studied in school.

We need diverse thinking to question our assumptions, to keep us from falling into analytic traps. This spring, I told the IC Lesbian, Gay, Bisexual, Transgender and Allies Summit that inclusion isn't just about what's altruistically right. It's also about what the IC is about: integration.

It means having and using a widely-diverse workforce, and taking advantage of all those great intellects we have, while removing as many frustrations and distractions as we possibly can. So it's not just about what's right. It's about good business in our profession.

Each of these seven principles has been a part of the Intelligence Community I've known for more than 50 years. I believe, if we keep these in front of us, we'll do just fine as our community continues to evolve. That's why I wanted them written down – in one place – in the front of our defining strategy for the IC.

So, I'll stop here. I've talked about our new National Intelligence Strategy, about the enduring attributes and goals it has for our IC, and about the importance of putting our Principles of Professional Ethics out in front of our strategy.

Thanks for listening, and we'll take some questions.

###