Information Sharing, Dot Connecting and Intelligence Failures: Revisiting Conventional Wisdom

By
Russell Travers
Deputy Director, Information Sharing and Knowledge Development
National Counterterrorism Center

This paper, written in August 2009, was submitted to the Director of National Intelligence 2009 Galileo Awards Program. The Galileo Awards Program is an annual Intelligence Community-wide competition designed to encourage and recognize innovative workforce ideas that address current challenges and help shape the future of U.S. Intelligence.

All statements of fact, opinion, or analysis expressed are those of the author and do not reflect the official positions or views of the National Counterterrorism Center (NCTC) or any other U.S. Government agency. Nothing in the contents should be construed as implying U.S. Government or NCTC endorsement of the author's views. This material has been reviewed to prevent the disclosure of classified information.

> *The year is 2014. The Intelligence Community is ten years into its efforts to implement the Intelligence Reform and Terrorism Prevention Act (IRTPA). While change has been evident on many fronts, nothing was more closely identified with intelligence reform than information sharing; ever since the 9/11 Commission declared that "the biggest impediment to all-source analysis – to a greater likelihood of connecting the dots – is the human or systemic resistance to sharing information"[1], the two had been inextricably linked. And while we were pushing more electrons than ever before, dissatisfaction continued: in 2014, as in 2009, no analyst in the IC had effective access to all information; analysts in many parts of the Community complained that they couldn't get operational traffic or law enforcement information; we had little ability to do large scale processing of foreign and domestic data sets; our non Federal partners were still dissatisfied with the quality of information sharing. A dizzying array of directives had been issued. Arbitration procedures had been established. And yet organizations weren't getting the information they claimed to "need." Legitimate issues coexisted with tripe. According to the critics, we still couldn't connect those dots. The reality, however, was far more complex: the only question was whether it took a major intelligence failure to realize that fact.*

This is the path we're on. We will continue to hear claims that information sharing has "barely improved since 9/11." Such hyperbole is unmitigated nonsense. The robust sharing of information between and among the key organizations has undoubtedly contributed to the fact that we haven't suffered a major attack. And by any objective standard, the level of sharing

[1] The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States; U.S. Government Printing Office. P. 416.

across the entire Government has increased dramatically. Building on robust IT architectures, Department and Agency access to information has reached unprecedented levels. Video teleconferencing has become broadly utilized as a means of quickly bringing appropriate levels of the Community together, and ensuring deliberation and situational awareness. More products are reaching more consumers than ever before. And increasing use of social networking capabilities are enabling collaboration and further stitching the IC together. Moreover, business processes have changed. More reports officers disseminate ever increasing amounts of information and make it widely available to the entire Community. Collaborative, multi-seal products are routinely produced. And we have dramatically improved our rapid "cascading" of information – from highly classified products drawing on the most sensitive sources and produced in hard copy, to perhaps a Top Secret ORCON version to a Secret NOFORN version to an allied releasable version to, perhaps an FOUO version.

To be sure there is work to be done, but why the level of intense dissatisfaction? This article will attempt to answer that question, and then suggest some concrete steps that could assist the intelligence community in improving on the sharing of appropriate information to support the full range of analytic missions and, at the same time, establish the "good Government" balance between and among such critical factors as sources and methods, U.S. persons' privacy rights, operational considerations, etc.

Retracing our Steps: Some Context

Our problems began with a woefully imperfect metaphor. Ever since the 9/11 Commission, the phrase "dot connecting" has been used as a popular shorthand description of what the Intelligence Community needs to do. It's a superficially attractive notion that would seem to suggest that if we just made all the information available to all the analysts they could discover the threat; after all that's the conventional wisdom about 9/11. As noted in the box, it's a conventional wisdom that is only partly true. Moreover, on deeper reflection the flaws in the dot connecting metaphor are readily evident. It conjures up the notion of the puzzle popular with five year olds – trace the readily identified numbers from 1 to 29 and find the outline of a duck…. Or in our case, the next terrorist plot, proliferation network, nuclear weapons development, or other threat du jour. Sounds straight forward, but in reality intelligence analysis

Fixing 9/11 Watchlisting Problems

There were undoubtedly information sharing shortcomings in the period leading up to 9/11, but the alleged poster child – failure to watchlist Khalid al Mihdhar and Nawaf al Hazmi until 24 August 2001–had more to do with a broken screening system than with information sharing shortcomings. At the time there were 4 classified data bases of known and suspected terrorists and 13 watchlists – these lists were neither broadly accessible nor interoperable. Failure was systemically inevitable.

Now, all USG terrorist identities information is maintained in a centralized classified repository at the NCTC and a derivative unclassified central watchlist is maintained by the Terrorist Screening Center. The relatively seamless flow of information across the USG means that CIA information collected in Pakistan can be used by State VISA officers in South America… that NSA collected information from SE Asia is utilized by DHS inspectors on the US/Canada border… that FBI collected information in the U.S. can be used to keep people off airplanes in Europe… and that DoD information from Iraq and Afghanistan can support traffic stops in downtown Baltimore. Or, any combination thereof. Yes there are inherent limitations in a names based system and yes, we are always working to improve the quality of the data base (with biometrics for instance), but the business process – establishing clear roles and responsibilities and building centralized data bases as an exercise of common concern for the entire government, shared with the appropriate organizations, reflects the kind of foundational work upon which true integration can occur. Fix the business process and information sharing followed easily.

has never worked that way. We may be able to pull the string on a threat stream and follow the "dots." But what if we don't know the outlines of the plot? How do we go about connecting the dots? Moreover, the nature of the information itself devalues the very concept of dot connecting. We don't actually know what information may be relevant to a particular problem and it's inane to think we can make "all" information available to "all" analysts. Some of the dots, for reasons that will be explained below, certainly won't be broadly available. And while some of the information – some of the dots – are legitimate, many others – particularly in terrorism, are often completely erroneous – some combination of lies, bad memories, misconstrued actions, hearsay, poison pen, etc. We often see the wrong dots getting connected and inappropriate warnings issued. The disconnect between reality and the rather stylized notion of dot connecting is huge.

But never mind. Driven by the need for a simple, easy to understand metaphor, we bought into the notion of dot connecting as a short hand description for an infinitely more complicated analytic function. We then overlaid the IRTPA as the legislative fix that, among other things, would allow us to properly connect those dots. The IRTPA certainly added some entities (a DNI, NCTC, among others), but otherwise left the pre 9/11 IC structure pretty much in place; each of the dozen or more organizations in the Community (and increasingly many outside) had independent analytic components, and they all had their own legislative mandates (explicitly protected by Section 1018 of the IRTPA). The multitude of analytic elements all had one thing in common – they asserted the self identified "need" for more information to do their job. In theory that shouldn't be a problem. Since the 9/11 Commission had decreed that information sharing problems were really all about "human or systemic resistance," the IRTPA established DNI could beat heads and direct that sharing. Hold that thought.

Meanwhile, the world in which the Community needed to operate was growing ever more complex. The Intelligence Community is confronted with the most complicated world in human history as a result of the incredible complexities of globalization – where distinctions like foreign and domestic often don't mean very much, where we are heavily reliant on foreign partners, where source sensitivity in some analytic disciplines severely limits the ability to broadly disseminate information, and where all difficult (important) subject matters reflect complex interrelationships:

- Our ongoing 20 year struggle with information overload has been further complicated by the challenges of dealing with foreign and domestic information.
- Virtually all subjects of any significance are a complicated mosaic of social, economic, political, military, and technical components.
- Individual bad actors have it within their grasp to take actions that can have strategic consequences. Barriers to entry are low and, in effect, these individuals use globalization against us.
- And as the roles and responsibilities of our Executive Branch Departments blur, we find seniors across the USG interested in the same information. Everybody wants their organic intelligence elements to replicate the same analysis many times over.

How do we deal with such a world? In a perverse way the IRTPA painted us into a corner and substantially limited our options. Since the legislation preserved a far flung empire of

intelligence analysts and protected Department and Agency prerogatives, our only conceivable approach was to stitch the Community together and create an intelligence "enterprise." We certainly have the technical wherewithal to connect the organizations; and, in theory, we could use the ever expanding suite of social networking tools to create a flat structure across the USG and strive for the "wisdom of crowds." Indeed some advocates of the enterprise solution took the construct one step further–extending the analytic function beyond the intelligence community and including the ever proliferating number of "intelligence" offices within Non-Title 50 organizations. Could USG-wide dot connecting nirvana be within our grasp?

Perhaps with some subject areas the approach might work. After all, even in Sherman Kent's day he noted that 80% of all relevant information was unclassified. It's certainly higher than that today, and for the vast majority of information in many analytic areas we can pass virtually all relevant intelligence, unconstrained, to all corners of the Community. However, it's a simple statement of fact that the extent to which information is broadly available to the Community varies dramatically by subject matter. And in some critical subject areas, there will always be a relatively small quantity of information that is a "game changer" in terms of shaping accurate intelligence judgments. It is this information that continues to tie the Community in knots. In general, those analytic areas that represent hard target areas will be the most problematic – by definition, hard targets implicate more sensitive sources and more limited dissemination. This is particularly true for subjects that lie at the cross roads of globalization – transnational threats, those having a foreign and domestic component, and those that relate to law enforcement and intelligence operations.

And there's the rub. What we've found is that no bumper sticker helps with this kind of information. The technical ability to pass information vastly exceeds the legal, policy and security framework. To be sure we've generated laws, executive orders, intelligence community directives, memoranda of understand and information sharing guidelines–all in the hopes of giving substance to the "need to share" or the "responsibility to provide." But in reality, inconsistencies, differing interpretations, and/or alternative policy statements deemed to be on point, rendered them largely impotent on any of the hard issues. Clearly no one argues with the general proposition that prudently sharing information with appropriate organizations is a good idea. But which electrons go to which entities? Answering that question requires burrowing down into the muck, where everything is a balance of competing legal, security, policy, privacy and technical/cost equities. To be more specific, does anyone advocate widespread sharing of all U.S. persons' information? Of course not. Indeed we've seen many instances where organizations have gotten their hands slapped for inappropriately collecting and retaining such information. Well, how close must the "nexus to terrorism" be to allow sharing if there are US persons' issues? Not a self evident question. And of course if there are particularly sensitive sources and methods at play, then naturally we need to protect them; and indeed organizations have the statutory responsibility to do exactly that. What if the information is part of an ongoing law enforcement operation? Then we certainly don't want to either inadvertently blow the operation or prejudice the judicial proceedings; the information will be shared with some entities, but not the entire "enterprise." And perhaps other information came from a foreign government. And that foreign government limited the USG recipients of *their* information? Do we ignore their proscriptions? Of course not; we clearly need to honor their limitations if we want to continue receiving that information. And you mean there are legal limitations on some

information: Privacy Act… Bank Secrecy Act… FISA Court restrictions… a host of others? Presumably no one is advocating breaking the law so of course we need to abide by legal restrictions. And we've got some proprietary information from the private sector… or State and local authorities provided information but limited dissemination? Then of course we need to respect those constraints as well. In other words, the overwhelming majority of the hard questions have absolutely nothing to do with "the human or systemic unwillingness to share information." Welcome to the real world of information sharing.

LAYING OUT A WAY AHEAD

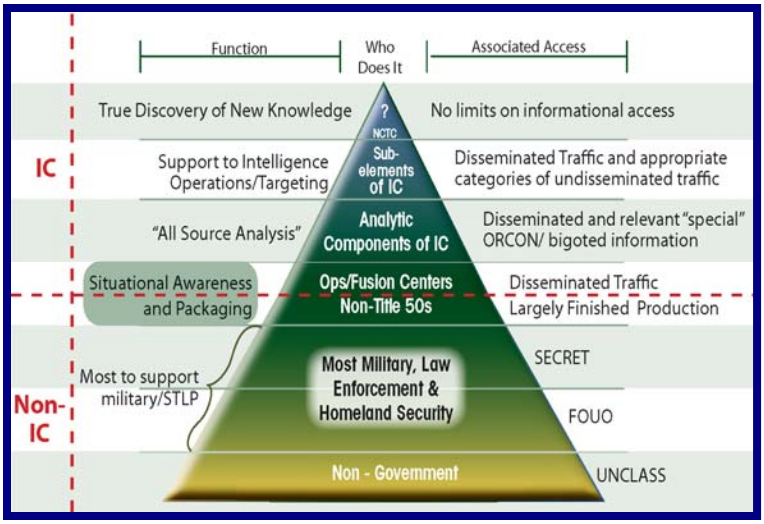
There's an understandable desire to simplify complicated issues; we have to make them digestible for busy overseers. As such, sloganeering has its place. But in this case we haven't done ourselves any favors. We bought into the slogans, opted to ignore those pesky complexities, and as a result we've gotten expectations way of whack with reality: we started with a woefully inadequate metaphor ("dot connecting"), bought into an overly simplified analysis of the problem (it's all about "human or systemic resistance to sharing information"), adopted a meaningless bumper sticker ("need to share"), failed to adapt to the challenges of globalization (interrelated problems that transcend foreign and domestic), fundamentally misrepresented the complexities of analysis (everyone can have an opinion on all subjects), exaggerated the potential of technology (the IC can simply replicate the "wisdom of crowds" approach) and failed to appreciate the legitimate impediments to sharing information (very real legal, privacy, policy and security reasons information should not flow). No wonder the period between now and 2014 is going to be painful. We never really understood what we were talking about.

So how do we regroup, build on the tremendous information successes we have had, and begin dealing with some of the extraordinarily hard questions that remain? The balance of this article focuses on three initiatives: first, suggesting a mission based construct that could be used to evaluate information access requests; second, addressing a very real gap confronting the community – the lack of an ability to do true discovery across foreign and domestic data sets; and third improving the quality of support to our non Federal colleagues.

ESTABLISHING A MISSION BASED FRAMEWORK FOR INFORMATION SHARING

The first major initiative focuses on a general delineation of roles and responsibilities – coming to grips with what "analysis" is and who does it. Why? Because, as noted above, we've spent the period since 9/11 mistakenly using "information sharing" as a way of avoiding hard discussions about mission – and therefore mission need. Clearly if everyone performs an all encompassing variant of "all source" analysis, then *reductio ad absurdum* they can (and often do) lay claim to "all" information. The Community (more accurately, the Government) has proven either unwilling or unable to clearly define mission space; more precisely we have mistakenly lumped together many different disciplines under the rubric of "all source analysis." Title 50, Title 10 and other Non-Title 50 organizations all assert the claim that they do "all source" analysis–and therefore they "need" all the underlying information. Clearly there's insufficient political oxygen needed to address the various legislative prerogatives at play, so the only alternative is to lay out general principles associated with who performs what aspect of

analysis (perhaps a worthy test of DNI authorities) – and using that construct to help guide who gets what information. These decisions would be informed by the various impediments to information sharing and could help the community pick the appropriate fights in addressing some of the very real, legitimate impediments.



A reasonable delineation of responsibilities and associated accesses could look something like that depicted in the diagram below, addressing from top to bottom, requirements for greatest to least access:

- The discovery function requires virtually unfettered access (to include ingesting of data sets into a repository to allow powerful tools to manipulate the data). While NCTC authorities come closer than any organization, no one in the USG is able to access all relevant foreign and domestic data (see initiative 2 below).
- Entities directly responsible for targeting, some law enforcement and intelligence operations need extraordinarily granular information – this implies accessing not only disseminated traffic but also being privy to relevant undisseminated operational and law enforcement information.
- The more typical "all source intelligence" organizations responsible for support to their Departments and Agencies should have access to finished intelligence, most disseminated traffic and select bigoted information as is directly relevant to their mission. Once and for all we need to dispense with the notion that "all source" means "all information;" it never has and it never will.
- Watch Centers and other organizations have largely a situational awareness function. In general their requirements will include discussing/sharing amongst themselves readily available disseminated traffic to ensure all organizations are on the same page.
- Non-Title 50 organizations with "intelligence" components that aren't part of the Community should draw largely on either Top Secret or Secret finished products, as clearances warrant, from the Community. They track IC judgments in the context of their Department/Agency mission. Again, a situational awareness function.
- Non Federal Law Enforcement, Homeland Security, and Private Sector officials will have access to either Secret or FOUO/Sensitive But Unclassified judgments, as clearances warrant, from the Community (see initiative 3 below)
- And finally the IC will make unclassified assessments to the American public in order to promote situational awareness and informed discussion.

In this construct the value of various social networking capabilities can be enormous. A relatively open free flow of Top Secret Originator Controlled (ORCON) information between and among a well defined category of "analysts" within the intelligence community can help

ensure open debate and allow various parts of a huge community to stay abreast of other's thinking. But it shouldn't be opened to everyone who simply self identifies as an analyst. And it can not replace the need for allocating roles and responsibilities; far too many data sets will never be available in A-Space or any other enclave that is broadly accessible.

DISCOVERY

The second major initiative builds on the first and establishes a capability for true "discovery" – in essence, an enhanced ability to connect dots when we don't have *a priori* knowledge that there is any relationship between/among them. The logic is both straight forward and unassailable. Terrorists, proliferators, international criminals, arms traffickers, foreign weapons developers - indeed all categories of bad actors leave electronic footprints when they identify themselves, travel, communicate, move money, etc. The data associated with those activities resides in a wide range of repositories, some open source, some transactional, some intelligence community, some law enforcement, some from other Governmental organizations (DHS and the Department of State to name just two key examples), and some from other private sector organizations; of particular import, some of these data sets by definition contain large amounts of U.S. persons-associated data and need to be treated with exceptional care. Do we have the technical wherewithal to process this data? Yes. Do we have the legal and policy framework necessary to guide this degree of data processing? No. Do we need the capability to comprehensively integrate and correlate this data? Here, reasonable people will undoubtedly differ in their answers. You can make a coherent argument, for instance, that we haven't been attacked since 9/11 and therefore we don't need any enhanced ability to uncover terrorist connections. On the other hand, there is no question that terrorists are getting more sophisticated in their ability to mask their activity and that further complicates the very difficult job of the terrorism analyst (or any other hard target analytic discipline). On one point there can be no argument – the lack of this capability does in fact represent a risk and it requires a serious conversation about whether we find that risk acceptable.

In the Event We Fail Again: The Ultimate Solution

While the initiatives in this article are hardly comprehensive, even they would stretch the bounds of political feasibility. Any real overhaul of the IC would only result from another intelligence failure so catastrophic as to reopen the IRTPA. What might IRTPA-2 look like? The original legislation provided a potential model with the creation of the NCTC; directly subordinate to the DNI, this interagency organization has greater access to terrorism information than any other element in the Community. IRTPA-2 could establish a large DNI analytic element that consolidated the Directorate of Intelligence of the CIA and many of Defense Intelligence's analytic elements. CIA would no longer have an analytic function and would be remissioned to focus on HUMINT collection and covert action. Similarly Defense Intelligence would be refocused on direct support to military operations. Generally Departmental and Agency intelligence offices would draw on commonly available intelligence, synthesizing and packaging information, and be responsible for ensuring broad situational awareness for their Departments and Agencies.

Anything approaching an IRTPA-2 of this scope and scale would involve a massive reallocation of authorities and responsibilities. The associated legislative, personnel, programmatic and IT implications of implementing such an overhaul would give "daunting" a whole new meaning. Hopefully a few modifications to our otherwise cumbersome, inefficient structure will see us through and we'll never have to find out how painful and disruptive such an overhaul would actually be.

To be sure there are multiple directives and data crunching initiatives that attempt to get at the discovery challenge, but they range from incomplete to inherently flawed – either they fail to understand how data correlation and integration actually works, or they fail to get to all the relevant data. Having visibility into the title of a document and then requesting discovery may help with some kinds of analysis, but it will do nothing to improve the kind of large scale data processing that could uncover terrorist linkages. Similarly, numerous Departmental and Agency large scale data processing efforts may get at part of the problem, but various security, legal, and privacy restrictions preclude a broader effort to comingle various categories of information – this gets particularly tricky when it comes to sensitive operational and/or undisseminated intelligence/law enforcement information, and even more so for data bases containing U.S. persons' information. As a result what we find are multiple Departments and Agencies trying to cut deals to get each others' bulk data stores – an incredibly inefficient, expensive and sub optimal proposition. This is an activity that cries out for centralization – an activity to be done as an exercise of common concern for the entire Government.

Importantly, this kind of work must be clearly distinguished from "pattern analysis". The goal isn't to identify activity that mirrors indicators of nefarious activity; that would almost certainly be a feckless exercise. Activities associated with preoperational planning for terrorist attacks, for instance, are almost invariably subtle and wouldn't lend themselves to this kind of analysis – the background noise would simply be too overwhelming and the potential for false positives would be huge. Instead this kind of large scale data integration and correlation would be intended to help find concrete connections to assist the intelligence and law enforcement communities (as well as Defense, Homeland Security and others). This interagency effort – presumably under the direction of the DNI and in support of Community wide activities -- would require massive computing power and analytic tools at its disposal.

It is inevitable that this effort would be assailed as a reincarnation of Admiral John Poindexter's Total Information Awareness (TIA). The parallels are evident, bringing computing power to bear against ever increasing amounts of data; and Poindexter was undoubtedly correct that technology was our only hope of ever processing such a deluge of information. But his effort was stillborn, suffering from a combination of secrecy, lack of trust, questions about business process, concerns about oversight, and disagreement about which data sets would be included. The TIA experience should teach us that any such effort must be an exercise in open covenants openly arrived at. Sophisticated discussions with the Congress, academics and the civil liberties community would be required. And if the effort were to go forward, the ultimate business process should include civil libertarians and lawyers sitting side by side with those doing the data processing. If the effort should be deemed politically unacceptable, however, such a decision should only be taken with a full understanding of the attendant risks – that lots of dots simply won't get connected.

SUPPORT TO STATE AND LOCALS

And the Third initiative would seek to improve non Federal access to appropriate information in a timely manner. Because most of our non Federal colleagues have no clearances the emphasis has traditionally focused on "tearlines" (a very brief unclassified synopsis of a classified document) and other unclassified assessments. For some issues this presents no

problem – much work can and has been done in the area of tactics, techniques and procedures associated with terrorism, for instance. And when general warnings need to be issued, they too can usually be done at the level of For Official Use Only, or Law Enforcement Sensitive. But unfortunately in many cases this approach is woefully inadequate. First, many organizations have been overly exuberant in responding to "need to share;" having been beaten up for not sharing they've provided information in tearline form that has proven either incorrect or incomplete. In other words sometimes we've shared too much information and the Federal Government has erroneously caused our State and Local Partners to unnecessarily take expensive actions. And secondly, even if the information is correct, an unclassified tearline is, by definition, a very crude instrument – it provides very little detail and context and can leave the recipient guessing as to how seriously to take the threat and how to allocate scarce resources.

To be sure the Government has gotten better – utilizing standardized context statements and being less predisposed to simply throwing information over the transom without having done a degree of vetting. Nevertheless only so much detail can be provided at the unclassified level. To partially compensate for this problem there has been a concerted effort to increase the availability of classified information at Fusion Centers and JTTFs. That's an improvement, as far as it goes, but there is a huge "last tactical mile" problem – an inability to get classified electrons to police departments, homeland security advisors and others that have a critical need to understand the underlying context behind a threat condition. There's simply no getting around the fact that in many instances this can only occur at the classified level.

As a matter of national policy we should adopt an appropriate technical/security solution that allows non Federal partners with appropriate clearances to "log in" on a classified lap top at their desks and review finished intelligence production. Some sort of proxy server maintained by FBI and DHS that provides the classified Community analysis relevant to our State and Local partners would be a dramatic improvement over the current processes. It is simply unrealistic to think that Homeland Security Advisors or busy police executives are going to drive to a Fusion Center, JTTF, Armory or other hardwired location to read Community judgments. Select homeland security officials and law enforcement need to be able to access materiel from their desks. Clearly we have the technical wherewithal to encrypt electrons and pass such material. And yes, we'll need an ability to audit use and the policy/training/security/cost issues will be significant. But we simply have to get past the intellectual logjam that says unclassified "tearlines are the answer."

Conclusion

The Intelligence Community has made extraordinary progress in the realm of information sharing. The low hanging fruit is largely gone and we're now confronted with some very difficult and very emotive issues. Broadly speaking this article has argued that we're approaching them in the wrong way. First, we emphasize information sharing rather than first getting our roles and responsibilities straight; it's a cart and horse problem -- we need to address "who does what" before we address "who gets what." Second, we're trying to level the "enterprise" (ORCON for everybody[2]) rather than first insuring that the Community actually can

[2] Make no mistake, the more the Collectors sense that legitimate constraints on information are being violated and their sources placed at risk, the more they will put information into harder to reach repositories

do discovery; we have a huge hole in our capabilities that needs to be addressed. And third, we're too focused on unclassified support to our non Federal partners and we need to accept that increased access to classified information has to be part of the solution. The three initiatives laid out above attempt to build on the Community's exceptional progress in information sharing and further the ultimate goal of the IRTPA – to strengthen the Intelligence Community and help make the Country safer.

One final point. In a sense, the focus on information sharing begins to pick at a far more fundamental issue. What exactly do we mean by the "Intelligence Community" and what is our role relative to all the other entities across the USG that do "analysis." If we buy into the notion of an "enterprise" and a relatively free flow of information between and among Title 50, Title 10 and other non Title 50 organizations, what are the implications? What about intelligence oversight? Is it "good government" for relatively "raw" information to be passed all over the national security apparatus? There is clearly a blurring between intelligence and operations – and that extends to a blurring between intelligence and policy. That certainly argues for robust information sharing, but it also presents some huge challenges. At the most fundamental level the intelligence community is charged with providing objective analysis and keeping the policy debate intellectually honest. The more "raw" intelligence is made available to policy makers the more inclined they are to create their own "intelligence shops." One doesn't need to go very far back in history to see what can happen as a result. We certainly shouldn't be afraid of defending ourselves against alternative views; but if policy makers opt to work around the Intelligence Community and to use their independent assessments to slant the policy discussion the integrity of the system is undermined.

In sum, the information sharing agenda ahead of us implicates everything from the definition of analysis, to the nature of the Intelligence Community, to how we as a free people think about privacy. There's no question that the technical wherewithal to share electrons and the associated policy framework are badly out of sync. One wonders whether the view from 2014 will be any better.