Remarks by the National Counterintelligence Executive
Dr. Joel F. Brenner

4th Annual Multi-INT Conference
Institute for Defense and Government Advancement

Sheraton Premiere
Vienna, Virginia

February 24, 2009

AS PREPARED FOR DELIVERY

DR. JOEL F. BRENNER: Thank you for the opportunity to be here this morning to discuss the unique difficulties of information sharing in the intelligence community. I work for Dennis Blair, the Director of National Intelligence. The DNI's mission is to integrate the nation's intelligence activities, and I do the same for counterintelligence.

I said that our situation is "unique" because we are the people who, *by law*, must keep certain information secret. That is, by law we must to a significant degree remain opaque. Yet we also have to provide information to a wider and wider audience outside the intelligence community but within the government, and in some cases outside the government. That is, by mission requirements and by policy, we must to a significant degree be transparent – *to a selected audience*. Managing this tension is what I'm going to talk about. It's a CI and security challenge of the first order, and meeting it requires us to do what in our sound-bite culture is a rare thing: That is, to keep more than one important idea in our heads at the same time.

But before I launch into that, let me explain what counterintelligence does. Counterintelligence is the business of identifying and dealing with threats to the Untied States from the intelligence services of foreign states and similar organizations of non-state actors, such as al Qa'ida and the Lebanese Hizbollah. We have both a defensive mission — protecting the nation's secrets and assets against foreign intelligence penetration — and an offensive mission — finding out what foreign intelligence organizations are up to in order to better defeat their aims.

Counterintelligence is not security, however. Let me put it this way. If there's a hole in your fence, security's job is to fix it. Our job (in part) is to figure out how it got there, who's been coming through it, and what they took when they left. And how to return the favor. We collaborate closely with security, but we're in a different line of work. The part about "Who's been coming through…the hole in the fence" refers to the very serious business of catching spies, or counter-espionage. But that's only part of our job.

21st Century Counterintelligence

Counterintelligence today is a broader, more complex undertaking than counter-espionage, though counter-espionage will always be our core concern. That's because when you create, store, and transmit information electronically – as we all do – you can also steal it electronically. Network and data security have therefore become CI problems. If you can steal information or disrupt systems electronically from thousands of miles away, why run a spy or saboteur? In fact, our public and private information systems and infrastructure control systems are under constant attack. And I emphatically include systems run by the Defense Department and our major banks as well as by public utilities that control our electricity grids. When I came to my post in 2006, I was startled to realize that the office was neither organized nor resourced to deal with network and cyber vulnerability. This is the new frontier of CI, so we fixed that pretty quickly. When it came time to write the CI part of the Comprehensive National Cyber Initiative, my office co-led the drafting with the FBI, which put up a senior to run our new section devoted to these issues.

According to the US Computer Emergency Readiness Team in the Department of Homeland Security, last year there were 5,499 tracked incidents of unauthorized access to US government computers and installations of malicious software. This is against 3,928 such incidents in 2007 and 2,172 in 2006. The trend is bad, and the US-CERT data almost certainly under-counts the problem.

We see the same trend in the private sector, where hacking for fun (Really, this is electronic burglary dressed up as a first amendment right) has turned into hacking for profit. I won't regale you with more stories of massive losses of personal data and privacy violations. Unless you've been living under a rock, you know about that. I'll just point out that cyber crime is now a mature business model with a well-developed secondary market for electronic burglar's tools and stolen information. And as the market for stolen personal data has become saturated, the emerging target is corporate intellectual property.

Just a few weeks ago McAfee, the firewall maker, reported that the average company surveyed world-wide has $12 million worth of sensitive information residing abroad, and that in 2008, companies on average lost $4.6 million worth of intellectual property. According to McAfee, "The global economic crisis is poised to create a perfect information security risk storm, as increased pressures on firms to reduce spending and cut staffing lead to more porous defenses and increased opportunities for cyber-criminals. Forty-two percent of respondents interviewed said laid-off employees are the biggest threat caused by the economic downturn."

Threats are both external – intelligence services, criminals, terrorists – and internal: not only disaffected or laid-off employees, but also spies and – please note this – careless employees. A leak of government or corporate secrets caused by an employee who unwittingly introduces an electronic vulnerability into your system has exactly the same effect as a vulnerability that's put there intentionally. And in fact we are seeing foreign intelligence services plan cyber operations that key off sloppy employee network behavior and sloppy network management practices.

And so we in counterintelligence now face a range of challenges that include but go far beyond the age-old problem of rooting out spies and traitors.

The Information Sharing Problem

That's the world we live in. That's our context. Now let me return to my theme, which is managing the tension between sharing information and keeping secrets. I want to be perfectly clear on this: As an intelligence community, we will rise or fall on our ability to move important and often secret information to those who need it, and to do it swiftly. But unless we do it very carefully, we run the danger of undressing ourselves electronically faster than our adversaries could do it to us.

The intelligence and law enforcement communities were faulted in the wake of 9/11 for failing to share information that could have made our tracking of the al Qa'ida threat more effective. As a result, information sharing evolved rapidly — and in some cases haphazardly. The legislative mandate stimulated rapid development of systems requirements to field new means of sharing information broadly and rapidly. Unfortunately, we have not paid enough attention to the operational and CI implications of the rapid deployment of information systems.

That evolution started with Congress directing greater emphasis on intelligence sharing in the 2004 intelligence reform legislation. The commissions that reviewed the 9/11 attacks and related emergent threats, like the proliferation of weapons of mass destruction, did likewise. These mandates were then reflected in strategic planning documents like the National Intelligence Strategy and the National Counterintelligence Strategy. They're now official policy. Finally, they influenced innovative technical developments, taking advantage of COTS and open-source solutions, to foster improved collaboration, especially within analytic and counterterrorism organizations. I won't mention specific systems; this audience knows what I'm talking about.

That's all good, but unless you propose to share every *thing* with every *body* – and *nobody* proposes to do that – you've got to decide what to restrict, whom to restrict it to, and how to restrict it. Whether you call this need to know or whether you call it something else, this problem is inherent in the business, and it cannot be made to go away by waving a wand or reciting slogans. And by the way, a policy decision to this effect is merely the beginning, not the end, of managing this dilemma. Systems must be engineered and operated to implement that policy. That is difficult, and it is expensive, but it is essential if we are to move beyond a battle of slogans ("need to know" vs. "information sharing") – essential if we are to have a serious discussion about the real challenge, which is information *management*.

Now I know that program managers eager to meet information sharing mandates sometimes object to security requirements they may see as impediments to the free flow of information, and they pressure their own developers accordingly. But in my experience, persistent and reasoned arguments will win out. Not to mention the salutary and embarrassing effect of disclosing recently introduced vulnerabilities. (Yes, reason is good and persistence is essential, but there's nothing like the prospect of embarrassment to move a bureaucracy.)

By the way, I don't want to suggest that the information sharing side of this dilemma has been solved. *Dilemmas are never solved; they must be managed.* We still find information that doesn't move when and where it should. We have made enormous strides in dealing with that

problem, however. It's a problem that arises from the natural tendency of collectors to hoard information. That's a cultural problem in a specific section of our community.

The careless sharing of information – frankly, the creation of unintended electronic vulnerabilities – is also a cultural problem, but it's a different cultural problem, and we find it in a completely different part of our community: among the technical propeller heads. Among whom it is a bedrock but rarely examined article of faith that if you can do something, you should. Because it's cool to connect stuff and create new capabilities. Remember, we recruit a creative and motivated technical workforce from the same labor pool that Verizon and Best Buy recruit from. Among this group, openness, not secrecy, is the watchword. (I will add that America is great because of its openness, not because we are secret. We in the intelligence business are in a line of work that rests uneasily in a democratic embrace.) Getting this sub-culture to understand that we in intelligence are sworn by oath and obliged by mission *and law* to keep some things secret is a serious and counter-cultural challenge.

Our last disaster on 9/11 was arguably caused by a failure to move information where it should have gone. The next disaster could well be caused by our relentless push to move information before we understand where it's going, only to find later that we moved it right into the lap of a hostile foreign intelligence service or terrorist organization. We Americans are a trusting lot. We are not born with an inclination to protect secrets, and an exhibitionist culture does not inculcate it. Quite the contrary. We have to teach it and re-teach it to each succeeding generation of intelligence officers and especially to the technical cadres that support them.

This is not a government-only challenge. It's a challenge for every organization with secrets to keep. Training and earning the loyalty of your employees is hard and important work, and as the McAfee study I mentioned earlier suggests, this is perhaps a bigger problem in the corporate world than in the government.

A year or so ago I was addressing an audience of entrepreneurs in Silicon Valley. What they wanted was for me to tell them what black box they should invent to make the cyber vulnerability problem go away. The answer is: *There is no black box, real or imagined, that can make this problem go away.*

Segment vulnerability and you'll understand why. We have three kinds: (1) technological, (2) management, and (3) behavioral or cultural. Of the three, behavior and culture are by far the hardest to deal with. Sure, we have some technological challenges, but failure to implement available technology – which is a persistent issue -- is not a technological problem. It's a management problem. And dealing with our workforce's relentless demand for convenience, and its impatience with reasonable security requirements – that's a behavior problem. As you may have noticed, whenever convenience and security butt heads, convenience wins hands down, every time.

This is why you can't simply mandate behavior and assume your mandate is being carried out. You can't slap the electronic equivalent of a yellow sticky on a system saying Do this, or Don't do that, and expect compliance. Nobody pays attention. If you don't want people to be able to execute a certain function, your systems have to be engineered to prevent it. If you want to

permit a function only in certain circumstances, then you must prevent its execution unless an authorized person approves it – and you've got to have an audit trail. Unfortunately it's necessary to add that having audit trails serves no purpose unless somebody actually performs an audit. I'll say categorically that an information system that is not subject to rigorous and periodic audit is a system that's in trouble or that will cause you trouble.

Ladies and gentlemen, there's a sub-theme here: *You can't make effective rules for behavior (whether it's information sharing or anything else) unless you understand the technology on which the behavior rides.*

Let me give you another example. As you know, there are by statute only three types of classified information: confidential, secret, and top secret. But at the top-secret level we also have horizontal categories called compartments and special access programs. If I delegate the architecture and management of an information system, my delegate is now the real SAP *meister*, the gate-keeper – *regardless of what the rules say.* And if that delegate designs or administers the system to permit persons to post compartmented information to it, while at the same time giving access to users who are not in the compartment, my delegate will have destroyed the compartment, possibly without anyone realizing it. I assure you this is not merely a theoretical problem.

And that is why we in the counterintelligence business find ourselves so deeply concerned with information systems.

When Christopher Boyce betrayed America in the 1970s, he carried out classified documents hidden in his clothing and, in one case, in a potted plant, to turn over to his accomplice, Andrew Daulton Lee, and to the Soviets. By the time Rick Ames betrayed us a decade later, he used a combination of hardcopy and downloaded information on discs. Still later, Robert Hanssen's computer literacy compounded the damage he did to FBI networks and our national security. Now, you can walk into many corporate and government offices, slip a thumb drive into an open USB port, and download in seconds more information than all these traitors stole together. We've come a long way from Whittaker Chambers' stuffing information into a hollow pumpkin.

Information transmission and storage have advanced to the point where the insider threat doesn't even have to involve a willful act by a determined traitor. Consider the wireless world and last year's Beijing Olympics. Your phone or Blackberry could have been tagged, tracked, monitored, and exploited between your disembarking the airplane and reaching the taxi stand at the airport. And when you emailed back home, some or all of the malware may have migrated to your home server. This is not hypothetical.

Your cell phone? It's a great device for sharing information. But the mike can be turned on when you think it's off.

Your iPod? It would be nice to have in classified spaces, but it's also a recording device. The ear buds work real well that way. Or didn't you know that?

Thumb drives? They're the electronic equivalent of unprotected sex and the biggest source of what I call ETDs, or electronically transmitted diseases.

Don't worry, I'm not telling you to abandon these dandy devices. Inexpensive electronics have brought us massive productivity gains and convenience. It is time, however, to take a deep breath and understand the vulnerabilities they have created. These devices do things most people don't understand. And that fact turns perfectly loyal but unwitting or careless colleagues of ours into walking vulnerabilities. Maybe most people don't need to know about that stuff. But if you handle sensitive information, whether it's state secrets or your bid numbers on a construction contract, you do need to know. As I mentioned, foreign intelligence services are now creating attacks on our systems that are based on exploiting these vulnerabilities.

In my view, we cannot responsibly discuss information sharing without reference to these unpleasant aspects of our electronic and cultural environment.

Information Sharing and Decision Advantage

To be sure that I am not misunderstood, I'm going to reiterate that much intelligence value today arises from how fast we can gather, understand, and move information to create decision advantage for our civilian and military leaders – not by how much of it is locked in a safe. That advantage can accrue to our economic or political competitors or to terrorists as much as to us, however, so we've got to be better at this than our competitors and our adversaries.

Notice that I'm talking about information, not just secrets. There are contexts in which the distinctions between bits, bytes, data, and information are essential, but the distinction one sometimes hears between intelligence and information is spurious. It feeds the fallacy that Intelligence (capital "I") is necessarily secret or top secret – that this is the only stuff worth paying attention to.

We also need to manage and share information – and facilitate the ability of the dispossessed to do so – in order to exercise our substantial soft power, to use Joe Nye's phrase. Think of the impact of mobile phone technology in an African village, for example. Imagine the opportunities it creates. Connecting people increases freedom. In the short run it doesn't always create stability, but in the long run it makes a better world. This, too, is an aspect of information sharing.

You've asked me to speak today about information sharing, and I've tried to do it in ways that stimulate thinking. Slogans are bad for thought, and this one is no exception. When it comes to how we deal with information in the intelligence community, it is far better, in my view, to think and speak about information management.

The national security partnership among government, industry, and academia will help us achieve responsible information sharing in service to our nation's strategic interests — winning the soft-power struggle, protecting America, and preserving our decision advantage in civil and military affairs. Dialogues like this one here today are essential in fostering that partnership, and I thank you for the opportunity to contribute to it.