Comments by William J. Lynn
CEO, DRS Technologies, a Finmeccanica company,
and former U.S. Deputy Secretary of Defense

Defense Security Services
2013 Foreign Ownership, Control or Influence (FOCI)
Facility Security Officer Conference
Wednesday, March 27, 2013

"Leveraging Global Defense Technology"

Thank, you Stan (Sims, DSS Director). You have taken DSS to a new level, further defining its mission and purpose. Partnerships with industry are now deeper under your leadership, providing us with more operational flexibility in return for greater transparency.

Thank you to all of the Facility Security Officers (FSOs) here today for everything you do to protect the nation's technology secrets. Today we salute you, the FSOs on the front line when it comes to protecting U.S. defense technology and information. Thank you for your service to your country.

The fact is that the use of global solutions to meet U.S. defense challenges is nothing new. And there are signs on the horizon that as defense budgets grow smaller, and the industrial base presumably shrinks, the need to leverage global technology and resources to address U.S. needs may well increase.

Historic examples of deep allied partnerships, extending from the battlefield to the factories and laboratories, are numerous. The Allies shared the secrets of the most important and elaborate military campaigns in history, from D-Day to Desert Storm.

Sharing sensitive information, and collaborating on defense technology, has always been a natural outgrowth of our alliances. My current and former companies are examples. During World War II, Raytheon partnered with a British electronics company, A.C. Cossor Ltd., to develop and mass produce radar, of life-or-death importance to the British during the Battle of Britain. During the Vietnam War, AgustaWestland − like DRS today a part of Finmeccanica − manufactured Huey helicopters at their plant in Italy, to increase production for Bell Helicopter. To underscore the depth of the personal relationships, inside Count Agusta's office, largely left in place today as a museum after his passing, there is a picture on the wall of Harold Bell, the founder of Bell Helicopter.

Allied scientists collaborated on perhaps the most Top Secret program of all time, the Manhattan Project to develop the atomic bomb. A British physicist, named James Tuck, directed the British mission at Los Alamos. Italian physicist Enrico Fermi's work on the first nuclear reactor and quantum theory earned him the nickname the "father of the atomic bomb" along with Robert Oppenheimer. Émigrés, including Danish physicist Niels Bohr and Austrian physicist Wolfgang Pauli, made Nobel Prize-level contributions.

Today, major development programs are underway among the Allies on some of the most critical front-line weapons platforms in history, especially the F-35 Joint Strike Fighter.

As the cost of development goes up, and budgets come down, globalization might only add pressure for technology interchange and collaboration on a scale yet unseen. When I was Deputy Defense Secretary, I cited three criteria that would increase DoD reliance on foreign or jointly developed technology:

- First, since the defense market is highly globalized, it is no longer the case that the U.S. has the corner on all the best technology. To maintain the most advanced military, we must buy the best products regardless of who develops them, us or our allies.
- Second, we need a global market to ensure competition across as many defense sectors as possible. Competition in turn brings lower prices and greater value. This reliance on a global market will become even more pronounced as stagnant or falling U.S. defense spending leads to further consolidation in the industry. To maintain robust competition, we need both domestic and foreign sources of competition.
- Finally, the U.S. should allow foreign defense companies into our market to better ensure that international markets are open to U.S. defense companies and products. Opening our market will not ensure that all markets are open to us. But closing our markets will certainly ensure that many more markets are slammed shut or remain closed. We have much more to gain than lose.

As we rely more heavily on a global defense market, the role of DSS to protect U.S. technology becomes even more central to our security. I run a FOCI company, DRS Technologies, which is part of the global Italian aerospace and defense company, Finmeccanica. In a recent brand analysis conducted by Finmeccanica, we learned that the best way for a FOCI company to gain confidence with U.S. customers is to demonstrate a commitment to security compliance and protect classified technology and information. Asked what the most fundamental requirement was, 56 percent of nearly 500 customers and stakeholders said the need to maintain security. Which means the greatest potential damage to your brand as a FOCI company would come from a major security breach. Think of a lapse in security as a potential death knell to your business.

Having a strong Compliance Program is a threshold requirement for FOCI companies. Moreover, a strong compliance program can help streamline the costs of doing business. Incentives are in place to encourage us to go above and beyond the baseline mitigation standards in return for greater operational flexibility.

For these reasons, at DRS we've worked hard to create a "Culture of Compliance." We strongly encourage reporting of suspicious activity. DSS has lauded our reporting process, which has given the agency even greater confidence in our security procedures.

A "Culture of Compliance" can only be developed from strong leadership from our FSOs. Business leaders need FSOs to foster and nurture three sets of partnerships. One set is with our employees. Another set is with our Government Security Committee. And

the third is with the people of DSS.

The members of the Government Security Committees are the recognizable guardians of America's secrets, respected and trusted leaders in their respective fields. They are the guarantors that FOCI companies will implement procedures and organizational changes to maintain strong compliance programs. We count on our FSOs to facilitate a free-flow of information to and from our GSOs.

We also count on our FSOs to strengthen our partnership with DSS. DSS has responsibility for nearly one million cleared contractor personnel in more than 13,000 cleared facilities. The agency fields tens of thousands of suspicious contact reports and participates in hundreds of investigations each year. From their perspective, companies with strong compliance programs lighten the government's load while strengthening security.

No one wants compliance programs to become so burdensome that the weight of it discourages foreign investment in the U.S. In fact, DSS is chartered with two compatible goals. One is to protect U.S. classified technology and information. The second is to facilitate a friendly U.S. procurement environment for foreign-owned defense companies.

In this context, DSS recognizes that they can help us simplify our operations. They can work with us to shape and tailor a customized compliance program to fit our company's size and unique environment. No two FOCI agreements are alike. A small company may need a greater connection to the parent for resources dedicated to security. A larger company may have a greater capacity to use automated reporting and training tools. More visibility into the day-to-day interactions of cleared employees could translate into greater flexibility to conduct business.

FOCI companies also can learn from the experiences of DSS. As the threat continues to evolve, DSS can help us keep pace. These days, it is not just about knowing the signs of suspicious behavior. Or what outlets employees have to report suspicious activity, from hotlines staffed around-the-clock to an "Open Door" management policy. Today, it's increasingly about the hidden threat buried inside our computing, data processing and IT systems.

The cyber threat extends beyond the need to protect sensitive and classified information and in fact has three dimensions:

- The threat to our military superiority from a potential adversary's own cyber capabilities;
- The threat to our critical infrastructure from destructive attacks on our power grid, transportation network, financial sector or telecommunications backbone;
- And the threat to our technological competitiveness, in both the defense and commercial sectors, from the theft of intellectual property.

On the last point, it is important to understand that nations have been stealing each other's technologies and military secrets for ages. In the Industrial Age, the Germans and the Americans stole manufacturing secrets from the British. In the nuclear age, the Soviet Union stole the plans for atomic weapons from us.

But the issue has changed with the advent of cyber technology that can increase both the volume of data that can be stolen and the speed at which it can be transferred and put to use by our adversaries. It is no longer possible to expect a buffer of time between the theft of information and its introduction into service. As a result, intellectual property theft has become not just an economic problem, but a national security threat as well.

Accordingly, DSS has a critical role to play. To be sure, as the security paradigm has evolved, cyber espionage has grown to the point where it is now the #1 threat. The numbers tell the story: cyber incident reporting to DSS increased by 76 percent in FY 2011 alone.

As you know, DSS has acted decisively. DSS established a Cyber Security Division to identify threats and reduce vulnerabilities. DSS signed an MOA with the Defense Information Systems Agency defining roles and responsibilities concerning contractor classified IT systems. DSS teams were trained to execute Command Cyber Readiness Inspections. Perhaps most importantly, the MOA presents a unified DoD face to the compliance community, simplifying the structure.

Let me talk more broadly for a moment about the challenges of cyber security. IT is now the fifth domain of warfare critical to military effectiveness along with land, sea, air and space. In context, warfare was first transformed by the industrial age, then by the atomic revolution and now by the information age. IT today is at the core of our most important military capabilities. It enables us to communicate with certainty, navigate with accuracy, see the battlefield with clarity and strike with precision.

Yet, the price for these increased capabilities has been to introduce new vulnerabilities. If our adversaries can compromise our networks, things reverse. They can blind our satellites, jam our communications, foul-up our logistics tail and make our smart bombs dumb again. Such an opportunity to reverse the advantages that we created through asymmetric attacks is not lost on our adversaries. Many are developing world-class cyber capabilities of their own.

As such, we must ensure that our military is able to execute its mission in a degraded cyber environment. We must ensure that our cyber networks have the highest possible protections, with the ability to hunt for intruders on our own networks. Since no defense is perfect, we must also have the offensive cyber capabilities to act as a deterrent.

To date, the most prevalent form of cyber attack has been those to exploit our networks and steal information. This kind of attack at first might not seem to have the same kind of immediate, destructive impact of conventional attacks. Yet, over the long run, the impact on our technological competitiveness and military superiority can be just as devastating.

In the last few years, a second type of cyber threat has emerged – the disruption of our networks. In these instances, intruders seek to deny or degrade the use of the network. The denial-of-service attacks against Estonia in 2007 and Georgia in 2008 were early examples. More recently, there have been similar denial-of-service attacks against commercial entities such as banks.

Yet, the third and most dangerous cyber threat is a destructive one, where cyber tools are used to attack and cause physical damage. This development, which marks a strategic shift, is just now emerging. Since the tools are readily available, it is clear that the destructive capability exists and will only grow.

As the cyber threat moves up the ladder of escalation, from exploitation to disruption to destruction, it is critical that the security community recognizes the threat and steps up to the challenge. As FSOs, you should know that adversarial groups that possess destructive cyber capabilities have been expanding in dangerous directions. We are moving from a world where sophisticated nation states once were the only ones with destructive cyber capabilities. Now, rogue states or even terrorist groups could develop or acquire them.

For all of you, that means that the people attempting to infiltrate our networks are not just nation-states trying to improve their own technological base by stealing U.S. secrets. It means the people trying to infiltrate our networks nowadays might later stage a destructive attack on the U.S. homeland or military. The reality is that your jobs will only get more complicated as the cyber threat grows, underscoring the need for government and industry to work closely together.

Today, we stand at a crossroads. Destructive cyber tools are being developed but have not yet been fully used. The most malicious actors have yet to acquire the most harmful capabilities. Our window of opportunity, to protect our networks against even more perilous threats, has an uncertain length. Which means the time to act is now.

Let me again say how thankful all of us are in industry and government for the work you do as Facility Security Officers. America counts on you to protect our most valuable secrets and assets. It couldn't be in better hands, of dedicated American patriots such as you.

Thank you.