James B. Comey

Director
Federal Bureau of Investigation

RSA Cyber Security Conference
San Francisco, California

February 26, 2014

The FBI and the Private Sector: Closing the Gap in Cyber Security

Remarks prepared for delivery.

Good afternoon. It is great to be here with you for what I hope will become a series of conversations over the next several years.

If you had told me a year ago that I would be standing here on this stage, talking to you about the FBI's capabilities to fight cyber intrusions, I would have said you were crazy.

Last year, I left Bridgewater Associates to teach law at Columbia Law School. I got to spend time with my wife and children, got to help out around the house. I wanted to learn to play the piano, get in good shape, read books I long wanted to read. Life was good…for a few months. In March, I received a call asking me if I would be willing to be interviewed for FBI Director. I told the caller that I didn't think so because it would be too much for my family, but I would think about it and call back.

I went to bed intending to call back in the morning and say "no." The next morning, I found my wife on the computer, checking out real estate in the D.C area. She said, "Look, I've known you since you were 19 years old. This is who you are and what you love." And then she paused for dramatic effect and said, "Besides, they're never going to pick you anyway." You can't put a price on that kind of support.

My wife, Patrice, in addition to being enormously supportive, has taught me a lot about life. She might argue it's because I have so much to learn. One of the most important things I've learned is the art of listening.

There are three kinds of listening. The first is what I like to call "Washington listening," which amounts to just nodding and waiting for the other person to shut up so you can say what you knew you wanted to say before they started talking.

The second kind of listening is actually paying attention to what the other person is saying—actually hearing their words.

It took me the longest time to learn that real listening—active listening—is a third kind. And it is a contact sport. You hunch forward, trying to pull information out of that person. You listen with an ear toward actually being convinced. You're saying, "I'm in this—I'm with you." And it is exhausting. But it is the real deal.

I've been meeting with folks in the FBI and with our state and local counterparts, and I've been doing a lot of active listening. My goal is to understand everyone's needs and to set expectations early in the game so that we are all on the same page.

My impression that the FBI is an incredible place has been confirmed over the past few months. We have folks all over the world, doing an amazing array of things—and doing them well. But, like all human organizations, we have problems. And we need to do a better job of listening to one another, to our law enforcement and intelligence counterparts, and to all of you to get a handle on our perspectives and what we need from one another.

I don't need to explain the cyber threat to you. You are the experts. You know we face cyber threats from state-sponsored hackers, hackers for hire, organized cyber syndicates, and, yes, terrorists. They seek our state secrets, our trade secrets, our technology, and our ideas. They may seek to strike our critical infrastructure and our economy. The threat is so dire that cyber security has topped Director of National Intelligence Jim Clapper's list of global threats for the second consecutive year,

surpassing both terrorism and espionage—even the threat posed by weapons of mass destruction.

Given the scope of the cyber threat, agencies across the federal government—including DHS, the Secret Service, and the Department of Defense—are making cyber security a top priority. Within the FBI, we are targeting high-level intrusions—the biggest and most dangerous botnets, state-sponsored hackers, and global cyber syndicates. We want to predict and prevent attacks rather than reacting after the fact.

FBI agents, analysts, and computer scientists are combining technical capabilities and traditional investigative techniques—such as sources and wires, surveillance and forensics—to fight cyber crime. We are working side-by-side with our federal, state, and local partners on Cyber Task Forces in each of our field offices. And we are training our state and local counterparts to triage local cyber matters so that we can focus on national security issues.

We are also working closely with our federal partners through the National Cyber Investigative Joint Task Force. Every key federal player is right there in one space—DHS, the CIA, the NSA, and the Secret Service, among many others—sharing cyber intelligence and working cases together. No turf battles or jurisdictional hurdles—just solid teamwork and collaboration.

Our legal attaché offices overseas coordinate cyber investigations and address jurisdictional hurdles and differences in the law from country to country. As you know, what is criminal here with regard to malware and intrusions may not be illegal overseas. We have special agents embedded with police departments in cyber “hot spots,” including Estonia, Romania, Ukraine, and the Netherlands, to identify emerging trends and key players.

But it isn’t enough.

We can’t do what we need to do without our private sector partners.

You are the primary victims of the evolving cyber threat. But you are also the key to defeating it. You have the information on your servers and your networks. And you have the expertise and the knowledge we need to stop these attacks.

We are actively listening to your concerns. We understand that you are reluctant to report intrusions, either because you're worried the government will start rummaging around your networks or because you fear your reputation will take a hit in the marketplace. You may be reluctant to share information with your competitors. You're worried about the loss of confidentiality and liability issues.

We don't always clarify what information we need from you, and you think it will take too long to provide it. There's no unified threat reporting system, and there is still some confusion about the "lanes in the road"—who is responsible for what in the federal government when it comes to cyber crime. How do you know who to turn to and how best to navigate the federal bureaucracy?

I get it. I know where you're coming from. I came to the Bureau from eight years in the private sector—five years as general counsel with Lockheed Martin, and three years with investment manager Bridgewater Associates. You have a responsibility to your shareholders and to the board. Your focus is on the bottom line. And then the government knocks on your door with a long list of requests and not a lot to offer in return.

As general counsel, I spent a lot of time asking myself—and my team—the same questions: "How come we can't get more information out of the government? How come they don't share information? Nations and criminals are trying to steal all our stuff; why can't they help us more?"

It often seems that the information flows just one way—to the government. Yes, we have information that we cannot always share. We are doing our best to change that. We need to share as much information as we can, as quickly as possible, and in the most usable format so that those of you in the private sector can take action. We need to continue to reduce our victim notification backlog so that you can take steps to

minimize any breach. And we need to clarify what we are looking for when you discover that you've been attacked.

We understand that you need to zealously guard your proprietary information and your customer data. We are surgical and precise in what we are looking for, and we will do what we must to protect your privacy rights and your competitive advantage. We want to work with you to figure out what happened and who was responsible so that we can better defend our networks and our data, identify emerging trends, and protect the public.

But we have to work together to see the whole picture. Look, I can patrol the street and say, "Hey, the street looks safe," but there are 50-foot walls on either side. And I can't see through those walls, and I can't get around them, so I don't know what's happening on the other side. We need your help to get past those walls, to protect you, and to do the job the American people have entrusted us to do.

We must provide the incentives, the means, and the assurances to share information quickly and routinely, as a matter of course. Effective partnerships are one way to do this.

The FBI has several great partnerships with the private sector already in place, such as the Domestic Security Alliance Council, InfraGard, and the National Cyber Forensics and Training Alliance. Many of you are familiar with these groups, and many of you contribute to their work. These partnerships are important. But we also need to cultivate one-on-one relationships.

Every special agent in charge of every field office should be on a first-name basis with key industry partners in their communities. And if they aren't, I need to know about it. If the SAC in your community hasn't reached out to you, take the initiative. As the old saying goes, the time to patch the roof is when the sun is shining. And it's cloudy at best out there.

We also need the means to share information in real time—machine-to-machine.

To date, we've been fighting DDoS attacks at mere human speed, sending malware indicators, host names, and IP addresses to those in the private sector. We understand that sending a laundry list of IP addresses without any context isn't useful and puts companies at risk of blocking legitimate web traffic. That's why we created the FBI Liaison Alert System—the FLASH—to send specific data used in an attack and that we believe will be used again.

We are providing ISPs with the information they need to shut down compromised attack nodes. And whenever possible, we have warned potential victims of pending network attacks so they can shore up their defenses.

But human speed won't cut it anymore. The cyber threat is too pervasive, too persistent, and too fluid.

Imagine a day where intelligence from combined sources—the government, anti-virus companies, ISPs, the financial services sector, and communications companies—is shared instantaneously, machine-to-machine, pursuant to law and with strong privacy protections in place. What if we were able to stop much of the malware as it transited the networks? It is no longer good enough to identify malware as it attacks your system.

We must be able to break down each intrusion into distinct phases. We need to create a blueprint, because even our most sophisticated adversaries will try to repeat successful attacks. We need to examine patterns and behaviors, to determine how they operate, and how best to stop them. We must build an intelligence-driven predictive capability. To do that, we need an automated intrusion system and a standard language and data format through which we all communicate in real time. And, of course, we need to do all of this while being mindful of the need to protect privacy and promote innovation.

But how do we get there?

We in the FBI have created a malware repository and analysis tool known as the Binary Analysis Characterization and Storage System, or BACSS, which provides near real-time investigative information. BACSS helps us link malware in different jurisdictions and paint a picture of cyber threats worldwide. Later this year, we will introduce an

unclassified version of BACSS, known as Malware Investigator, for use by all of our partners.

If your company has been hacked, you can send the malware to us, and, in most cases, receive a report within hours on how it works, what it might be targeting, and whether others have suffered a similar attack. Our goal is to make BACSS the nation's repository for malware and viruses, in the same way the FBI maintains fingerprints, DNA, and criminal arrest records.

We also want to provide a real-time electronic means for reporting intrusions. Through iGuardian, law enforcement and the private sector can quickly and easily pass information back and forth, both classified and unclassified. We can build on our collective knowledge and fight these attacks head-on.

This is the model we are striving for—using intelligence gathered from our own authorities and our own partners to stop a threat before it becomes a problem. This is the only true incentive we need—to prevent as many attacks as possible.

I want to touch on issues of privacy for a moment.

Some have suggested there is an inherent conflict between protecting national security and preserving privacy and civil liberties. I disagree. In fact, I think the ideas of "balance" and "trade-offs" are the wrong framework because they make it seem like a zero-sum game. At our best, we are looking for security measures that enhance liberty. When a city posts police officers at a dangerous park so kids and old folks can use the park, security has promoted liberty.

The men and women of the FBI are sworn to protect both national security and civil liberties. It is not a question of conflict; we must care deeply about both—in every investigation and every program.

The fact of the matter is that the United States faces real threats from criminals, terrorists, spies, and malicious cyber actors. That is reality. The playground is a very dangerous place right now. To stop those threats, the government needs timely and accurate intelligence to identify threat actors and to figure out what they are planning.

That means we need to conduct electronic surveillance and collect data about electronic communications. That is also reality. The real question is this: How do we do that in a way that allows us to prevent bad things from happening to our own people and our allies, and, at the same time, protect privacy and civil liberties and promote innovation?

I've never been someone who is a scaremonger, crying wolf—but I'm in a serious business, so I want to ensure that when we discuss altering tools we use to collect information on an individual we believe to be connected to criminal, terrorist, or other unlawful activity, that we understand the benefits and trade-offs on the other side. The same is true when we allow the effectiveness of those tools to erode gradually over time through the failure to update our laws, or when our tools become less effective through unauthorized disclosures of our capabilities.

Intelligent people can and do disagree, and that's the beauty of American life, but we need to make sure that everyone understands the risks associated with the work we do and the choices we make as a country.

The same considerations exist with regard to cyber security. Before he left, Director Mueller told me that he believed cyber issues would come to dominate my tenure as counterterrorism had dominated his time as Director. And I believe he is right. We must be agile and predictive on every front. And we must use every tool and authority at our disposal to stop these malicious activities.

The cyber threat is different than the terrorist threat, of course, because we have not yet experienced a watershed event like the attacks of September 11th, but we all recognize that we are at risk and that we must act quickly.

Look, these are tough issues. And there are legitimate questions and important things to discuss. I hope you know a bit about my history—I have dedicated my career to upholding the rule of law, and I am committed to making sure that people understand how the government is using its legal authorities. But finding the space and time in American life to understand these issues is very hard.

My hope is that we can resolve these issues through open and honest communication. That's my goal. It's my goal within the FBI, with our state, local, and international counterparts, and with all of you.

We simply must work together and play to our strengths. When it comes to cyber security, you have the technical expertise, the infrastructure, and the innovation. And you are often the first to see what's coming over the horizon. We have the intelligence and law enforcement capabilities and the global presence. We are each playing to our strengths. But even that isn't enough. We've got to play as a team.

It won't be easy. And we won't always see eye to eye. Basketball coach Phil Jackson—the so-called Zen master of the court—knew that each player held the power to make or break the team. In his words, "The strength of the team is each individual member. And the strength of each member is the team."

We need to figure out how to combine our strengths. And that will take time and a lot of active listening. But I'm in this for the long haul—I have a 10-year term. The FBI is in this for the long haul. We really are on your side. And we will do everything we can to keep your data, your innovation, and your intellectual property—not to mention your friends and families—safe and secure.

I look forward to working with you down the road. Thank you for having me here today.