Robert Boback
Chief Executive Officer
Tiversa, Inc.

Testimony Before the House Committee on Oversight and Government Reform

July 24, 2007

Good morning Chairman Waxman, Ranking Member Davis and distinguished members of the committee.

My name is Robert Boback and I am Chief Executive Officer of Tiversa, a Pennsylvania-based company that provides information technology and investigation services that help protect organizations, government agencies and individual consumers from the disclosure and illicit use of sensitive, confidential, and personal information on peer-to-peer file sharing, or "P2P", networks.

I wish to extend our most sincere appreciation for inviting us to testify on this very important issue today. And I also want to applaud the Chairman for calling this important hearing and this committee's previous legislation and work on this topic.

While the Internet is a true boon to our society and economy, there are critical personal privacy and national security issues that need to be addressed seriously, urgently and with the immediate intent to find solutions.

These privacy and security threats are caused by the inadvertent misuse of P2P file sharing software, which Tiversa estimates has been installed on over 450 million computers worldwide. P2P file sharing is one of the most powerful technologies created in recent years, however, as with the world wide web, it is not without inherent risks.

P2P technology provides an efficient way for people to share files with each other. Essentially, the technology uses the muscle power of the computers that it connects and allows people to share files directly with each other. When files are shared directly between two P2P users, this is called decentralized file sharing. This means the files do not go through any central computer server in the middle of the exchange.

P2P has gained both popularity and notoriety for the file sharing of entertainment content among its users. Yet, regardless of where one stands on P2P activity, it's unquestioned that P2P usage is rapidly growing and becoming generally accepted as the most efficient way to distribute large pieces of digital content to consumers.

Indeed, with the explosive increase in digital content including online video and user generated digital content, P2P file sharing is being embraced by many legitimate, well-known businesses to distribute and share television shows and full-length movies to consumers in a manner that protects the copyright and privacy of the content.

Therefore, P2P file sharing is becoming as much of a critical and integral part of the Internet's infrastructure as Web browsers are today. As a result, we must consider the privacy and security issues around it accordingly while allowing for legitimate uses of the technology.

Inadvertent file sharing happens when computer users mistakenly share more files than they intend. For example, they may only want to share their music files or a large academic report, but instead open all files on their computer's hard drive to access by other users on the P2P network. This typically occurs by a user error in either installing and/or using the software.

The result of inadvertent file sharing is hundreds of thousands of sensitive, confidential, and classified files are exposed and made available to the universe of P2P users each day.

Today, we would like to provide the committee with concrete examples that show the extent of how inadvertent P2P file sharing can negatively affect consumers, corporations, government entities and, indeed, our national security. During our testimony, we will provide the committee with examples that illustrate the types of sensitive information available on P2P networks, examples of how users on P2P file sharing networks actively search for inadvertently shared sensitive information, and offer our thoughts on actions to address this problem.

Despite the tools that P2P networks are putting into their software to avoid the inadvertent file sharing of private or classified information, this significant and growing problem continues to exist. Any changes made to the P2P software, while welcome and helpful, will not fully address the problem.

Warnings regarding inadvertent file sharing through P2P networks have been sounded in the past. The FTC has issued warnings on exposing private information via P2P mechanisms. The 2003 Government Network Security Act, co-sponsored by Chairman Waxman, Ranking Member Davis and several members of this committee highlighted the dangers facing government agencies and prescribed a course of action. Prominent security organizations, such as Carnegie Mellon University's Computer Emergency Response Team (CERT) and

the SANS Institute have warned corporations, governments, and consumers to the unintended dangers of inadvertent file sharing via P2P networks.

For example, CERT's *ST05-007-Risks of File-Sharing Technology - Exposure of Sensitive or Personal Information* clearly states:

> "By using P2P applications, you may be giving other users access to personal information. Whether it's because certain directories are accessible or because you provide personal information to what you believe to be a trusted person or organization, unauthorized people may be able to access your financial or medical data, personal documents, sensitive corporate information, or other personal information. Once information has been exposed to unauthorized people, it's difficult to know how many people have accessed it. The availability of this information may increase your risk of identity theft."

Additionally, many of the most popular P2P tools prominently display similar warnings to their users.

Regardless, the problem persists, and our opinion is that it's getting worse. Here is why we hold this opinion.

Beginning in 2003, Tiversa has developed systems that monitor and interact with and within P2P networks to search for sensitive information in an effort to protect the confidential information of our clients.

Tiversa centralizes what was previously a decentralized P2P file-sharing network. Tiversa can round-up all the previously untraceable activity on the network in one place to analyze searches and requests. Where an individual user can only see a portion of a P2P file sharing network, Tiversa can see the whole. It is our belief that no other system has this capability. We have the unique ability to observe activity across P2P networks, to see what inadvertent file sharing is taking place, and to see how P2P users are seeking this information, and where the information goes once it is shared.

Tiversa can monitor, on average, at least 300 million total P2P requests per day. We can investigate more fully to determine the intent of those requests. Our systems have the ability to record the searches for files made on P2P networks, as well as the ability to access the files available to users of P2P networks who issue these searches.

Users on a P2P networks must "ask" the network for a file before they can download them. For example, they may request "Frank Sinatra, I Did It My Way." That search request is then broadcasted to all connected users for a response that says in effect - "I have that song". At this point, the searcher can initiate a download request from their choice of users who possess that file.

Substitute the Sinatra search for "classified troop movements" and you begin to understand the problem. Or, if someone searches for "ABC Bank August Statement", we can deem their intent was to obtain bank statements.

For example, Tiversa set its algorithms to record P2P search strings that matched the term "Credit Card" and separately the term "Medical." Illustrated below is a limited set of English language examples taken from the millions of similar search strings that Tiversa observes each day:

Credit Card

▪ d&b credit card info	▪ credit card pin numbers
▪ corporate credit card log	▪ credit card with cv2 numbers
▪ credit card merch copy sr	▪ credit card statements
▪ davids credit card numbers	▪ credit card comm sept private
▪ credit card charge ctm costa	▪ credit card authorisation july
▪ credit card gateway ubc	▪ credit card app pdf
▪ 2007 batch of credit cards	▪ athens mba credit card payment
▪ cash credit card checks	▪ cathys visa credit card go on
▪ confidential credit card app	▪ credit card with acc
▪ credit card processing	▪ credit card statements

Medical

▪ dear medical insurance my	▪ child medical exam
▪ letter re medical bills 10th	▪ billing medical august
▪ denial of medical insurance	▪ digital files medical trans
▪ medical passwords	▪ authorizationform medical
▪ hospital records	▪ caulfield general medical
▪ comprehensive medical	▪ medical coding and billing
▪ medical release	▪ medicine medical passwords
▪ classified medical records	▪ isilo medical
▪ electronic medical record	▪ doctors office medical exam
▪ ltr medical maternity Portland	▪ medical abuse records

There are literally thousands of search strings that we can use to illustrate the millions of individual searches targeting sensitive information available on file sharing networks. One has to ask the question, "Why are P2P users searching for these files on a network typically used to share music and movies?" What are these users looking for? What will they do with the information once they find it?

We would now like to describe how consumers, businesses and government entities are victims of this problem by showing and describing actual examples of sensitive, confidential, and classified files inadvertently disclosed by these entities.

Individuals at Risk

P2P is a highly efficient way for a potential identity thief to gather an individual's private, privileged information that can then be used to commit ID theft, other forms of fraud, or put the individual's personal safety at risk. Yet, very few individuals are aware of this problem, let alone how to protect their information. There have been significant public awareness efforts aimed at educating consumers about phishing scams and other malicious activities. There has been very little effort made to protect consumers from inadvertently sharing information through P2P networks. Virus checking and firewalls, commonly highlighted as the solution, are not fully effective at solving inadvertent file sharing problem.

Examples of readily available documents Tiversa has been able to find on P2P file sharing networks include:

- Federal and State identification including passports, drivers licenses, and social security cards
- Dispute letters with banks, credit card companies, or insurance companies revealing account numbers, credit card numbers, insurance ID numbers and social security numbers
- Copies of individual credit check reports (e.g. Equifax Reports)
- Copies of individual bank and credit card statements
- Signed copies of health insurance cards
- Full copies of federal, state, and local tax returns
- Extensive electronic records of active usernames / ID's for online account access
- Wills and trust documents
- Mortgage and credit applications
- Life insurance applications
- Confidential medical history and records including psychiatric records
- Employment applications
- Family photographs and movies revealing children, addresses, and other personal information
- Student loan / aid applications and documents

Redacted examples that protect the privacy of individual document owners have been provided to the Committee.

In essence, whatever an individual stores on his/her computer electronically can be inadvertently shared. The impact of sharing these files not only hurts individual consumers directly, but also impacts the financial institutions, insurance firms, and government agencies who must incur the costs of fraud and investigations into wrong-doing. In these cases, consumers may hold these institutions responsible, when they themselves are exposing their own information. The lack of a mechanism to trace back to the source of the disclosure is often the issue in these cases. Fraud occurs, but consumers, corporations, and government organizations often do not know the root cause.

Corporate Breaches
Corporate inadvertent file sharing includes any entity that is not a governmental organization or an individual. No organization, regardless of its size or industry is immune from this problem. This ranges from the world's largest multi-national corporations across the financial services, insurance, defense, pharmaceutical, professional services and healthcare industries to small medical, accounting and law practices. Equally, no organizational function is immune to inadvertent file sharing. Tiversa has found files disclosed by and affecting human resources, finance, compliance, legal, research and development, sales, marketing, public relations, and the executive office.

With the increasing virtualization of corporate entities and the greater use of outsourcing, the concept of the *Extended Enterprise* has become critical to Tiversa's clients. This means that any entity entrusted with the corporations sensitive or confidential information can become a disclosure point on P2P file sharing networks. These entities include at home or virtual employees, contractors, suppliers, attorneys, consultants, accountants, or partners. These entities are almost always outside of the corporate perimeter and, therefore, outside of the direct control and enforcement of the corporation. How many times have you e-mailed a file home on which to work? Sent a confidential file to your lawyer or accountant? Inadvertent sharing over P2P file sharing networks is perfectly designed to exploit the *Extended Enterprise*. Our examples will show this.

As a matter of record, Tiversa observes searches similar to those previously illustrated for "credit card" and for "medical" for individual corporate names, subsidiaries, and acronyms. The illustration of these search strings would put these corporations at risk. The committee should note that the searches of this nature are every bit as aggressive and more specific as those for credit cards and medical information. In fact, many times we will see P2P users searching for specific file titles on a corporation. A recent example shows P2P users searching for a foreign exchange system design document for a major financial institution more than 40 times over a three week period. Tiversa knows this document is available since we obtained it as part of our work for a client.

The larger and better known a company and its brand, the greater the risks associated with searches for these corporations.

Tiversa has many examples of corporate information disclosures. Obviously, many are extremely sensitive and would put these corporations at significant risk if they were shared in a public domain. We are happy to share illustrative information with the committee in a secure environment if specific examples are needed.

The following, however, represents examples and situations that we have encountered illustrating the risk facing corporations today.

The first example illustrates a number of points relating to corporate disclosures clearly. Tiversa has discovered a third party attorney whose clients are the world's largest pharmaceutical manufacturers disclosing 436 sensitive and confidential files related those clients. The information covers, in part, pending litigation. One document, dated April 2007, is labeled "confidential" and "by hand" and addressed to Chairman Waxman with a carbon copy to Ranking Member Davis. It appears to address questions regarding drug trials of this pharmaceutical company. This is a case of an attorney who has exposed multiple pharmaceutical companies outside of their network – a clear example of extended enterprise risk.

A second case involves the exposure of the recent board minutes of one of the world's largest financial services organizations, and was disclosed by an executive assistant to one of the executive team members. This disclosure was originally found by a private investigator and reported to the corporation.

A third case involves the disclosure of the entire foreign exchange trading back-bone for one of the world's largest multi-national financial firms. These files were among hundreds of confidential internal computer design and security files. As we stated earlier, P2P users were searching for these by name.

A forth case illustrates how a contractor can expose a corporation. Tiversa observed P2P searches involving a contractor to one of our clients. Files exposed include the entire launch plan and expected growth targets for this diversified financial institution's entry into Europe. In addition, Tiversa observed these files in the possession of a P2P user in Nigeria. In this instance, a subcontractor to the initial contractor exposed our client's confidential information.

A fifth case again illustrates how a supplier can expose a corporation. Tiversa recovered the wide-area network and disaster recovery plan for a major banking institution exposed by the company to which the bank's entire trading network was outsourced.

Tiversa can provide literally hundreds of case examples like those illustrated above. In addition, we have found:

- Press releases in mark-up before their public release covering material, non-public information
- Patent related files before submission to the patent and trademark office
- Drug trial test records before FDA approval
- Legal documents including business contracts, non-disclosure agreements, term sheets, etc.
- Human resources related documents including employee reviews, executive recruiter post-interview write-ups, confidential termination and pending litigation documents, etc.
- Accounting related documents including audit reports, corporate tax records, payrolls, invoices, etc.

- Information systems related documents including administrative user ID / passwords to corporate systems, network diagrams, router access codes, functional specifications, disaster recovery plans

Highly select redacted examples that protect the privacy of individual document owners and any other sensitive information have been provided to the committee.

Given the media exposure that "lost laptops" and information disclosures on non-P2P networks has received, P2P inadvertent file sharing represents a significant brand, operational, legal, and regulatory risk to corporations. For example, a recent P2P sourced breach affecting 17,000 current and former Pfizer employees' personal information illustrates the impact of the inadvertent sharing of sensitive information on P2P file sharing networks. Any one of the examples provided to the committee could result in a similar problem for its respective corporation.

Classified Government Data Exposed
Inadvertent P2P file sharing affects all levels and branches of government, law enforcement, and intelligence agencies. For our testimony today, Tiversa will focus on how inadvertent file sharing affects federal government agencies and law enforcement.

As with corporations, government inadvertent file sharing may originate with the agencies themselves, contractors to these agencies, soldiers or agents in the field. The same "extended enterprise" exposure problem facing corporations faces the government.

In addition, Tiversa regularly sees P2P searches for government related information including classified information and searches that could assist law enforcement.

In 2003, Chairman Waxman, Ranking Member Davis and many members of this committee co-sponsored the Government Network Security Act. It was designed to quite simply: "require Federal agencies to develop and implement plans to protect the security and privacy of government computer systems from the risks posed by peer-to-peer file sharing."

In a press release announcing the Act, Ranking Member Davis was quoted saying, "Few people recognize these risks. Using these programs is similar to giving a complete stranger access to your personal file cabinet."
Unfortunately, while the bill passed the House, it stalled in the Senate. Now, four years later, there are hundreds, if not thousands, of examples of federal government classified documents publicly available on P2P networks at this very moment.

A stark example is the discovery of 34 classified documents available and found by Tiversa on P2P networks. At least one of these classified examples was

related to a government contractor. At least one of the classified documents is the secret property of the United Kingdom, which shows the inadvertent release of such sensitive data is unquestionably global in nature.

Prior to our testimony today, Tiversa provided secret classified documents we located to General Wesley Clark, an equity holding member of Tiversa's advisory board. He has since furnished these documents to the Chairman of the National Intelligence Advisory Board for investigation. This information could, and most likely does, pose significant risks to our interests domestically and abroad. Unfortunately, this is not an isolated incident.

Inadvertently shared information is not limited to classified information. A diverse amount of information exists across government agencies and contractors. Here are some examples:

1. A document illustrating over 100 individual soldier's names and social security numbers
2. Physical Threat Assessments for multiple cities such as Philadelphia, St. Louis, and Miami
3. A government contractor exposing an air force base physical security attack assessment
4. A document titled *"NSA Security Handbook"*
5. A detailed report from a well known government contractor for the National Security Agency (NSA) which outlines how to connect two secure DoD networks
6. Numerous Department of Defense Directives (DoDD's) on various Information Security topics – all signed by various Assistant and Deputy Secretaries of State
7. Various Department of Defense Information Security system audits, reviews, procedures, etc. (e.g. retina scanner equipment audits, penetration detection software/equipment reviews)
8. Numerous "Field Security Operations" documents including router checklist procedures, "Network Infrastructure Security Checklist", etc.
9. Numerous presentations for Armed Forces leadership on various Information Security topics including how to profile "hackers" and potential internal information leakers
10. Large numbers of army documents marked "For Official Use Only"

A case example illustrates the risks clearly. On July 17, 2007, Tiversa found a defense contractor employee disclosing 1,900 individual files from one IP address on P2P file sharing networks. This contractor supports 34 "Joint and Army agencies", including the Department of Defense at the Pentagon, Defense Intelligence Agency, National Security Agency, US Air Force, Army, Navy and the National Imagery and Mapping Agency. This person was disclosing a wide array of files including music, personal information, resumes, photos, etc. Alarmingly, this individual was also disclosing 534 files with extremely sensitive, privileged information regarding the US Government generally, and the Department of

Defense and various US Armed Forces specifically. The types of information disclosed included:

- The entire Pentagon secret backbone network infrastructure diagram including server/IP addresses
- Password change scripts for Pentagon secret network servers
- Department of Defense employees contact information (including cell and home phone numbers)
- Secure Sockets Layer (SSL) instructions and certificates allowing access to the disclosing contractors' IT systems
- A contract issued by the "Army Contracting Agency" at the Pentagon that authorizes expenditures in excess of $1.5 million with the disclosing contractor
- Numerous policies/procedures regarding the Pentagon's IT infrastructure as well as its threat response activities (including a "Draft Strategic Plan" for 2007 – 2011)
- A letter from a "Deputy Director for Management" at the "Executive Office of the President's Office of Management and Budget" which explicitly talks about some of the risks associated with P2P file sharing networks.

Ironically, it appears that the individual disclosing this information could be a member of a computer incidence response team and could hold top secret clearance – certainly not an uninformed computer user.

The risks posed by this disclosure source are widespread. For one, the disclosed information could be used directly to penetrate the Pentagon's secure IT environment in an effort to access highly classified information. Secondly, the information could be used indirectly against the disclosure source for blackmail, coercion, kidnapping, etc.

Outside of the alarming nature of this instance, this case clearly illustrates a number of key points:

- Extended Enterprise Risks – these disclosures appear to have happened *outside* of the Pentagon's network where traditional perimeter IT approaches and policies are not effective.

- One Source / Many Exposures – one source, in this case, adversely affected multiple government agencies. This exposure is worse than a lost laptop since P2P users have open access to the information on the computer without the knowledge of the owner. Anyone who knows what to look for can obtain this information and share it.

- Risk of "Open Windows" – whatever new files are now added to this individual's computer will then become available to the P2P user community. Despite the fact that sensitive files may or may not be

present on an employee or suppliers computer today, the very existence of P2P file sharing software can expose whatever files are added in the future.

Redacted examples that protect the privacy of the respective government agencies and affected individuals have been provided to the Committee with the exception of classified information which, as noted earlier, was provided to the Chairman of the National Intelligence Advisory Board by General Wesley Clark.

Law Enforcement Related Examples

Citizens expect our government to protect its own classified and confidential information, but to also enforce laws governing illegal uses and exploitation of information. Examples of this include enforcing copyright and licensing laws and export control laws. One example we wish to highlight to the committee is the extensive use of P2P Networks for searching and sharing child pornography. To illustrate the extent of this trafficking of this information, Tiversa collected searches that P2P users were issuing for known child pornography terms. This example is provided to the committee as a separate exhibit.

Live Demonstration

While the examples collected represent various periods of time, a glimpse into what is available *live* on P2P networks dramatically illustrates the extent of exposure for the categories of examples highlighted above. We will now show user issued searches and available files that match a select list of file probing terms.

Evidence of Wrong-doing

Tiversa has shown the committee live views of P2P user issued searches and available sensitive, inadvertently shared files. We have illustrated that P2P users are actively searching for sensitive, confidential, and classified information. We have shown sensitive, confidential, and classified files are present on P2P networks across individual consumer, corporate, and government sources. What happens to these files once they are found, downloaded, replicated, or used? Is there evidence of fraud or wrong doing?

Fraud Test

Tiversa, in conjunction with Dartmouth's Center for Digital Strategies, conducted a test to show that once a file with actionable financial information is inadvertently disclosed on a P2P network, individuals will use it for an ill-gotten financial gain.

Tiversa and Dartmouth purchased a VISA cash card and an AT&T calling card and incorporated the cash card numbers and phone card numbers instructions on how to use these into a letter. An electronic copy of the letter was put on a

Dartmouth test computer and shared using LimeWire file sharing software. Tiversa tracked the spread of the letter globally across P2P file sharing networks, from the point of initial compromise from the original source computer to its sharing and subsequent re-sharing(s). Tiversa and Dartmouth then tracked the real-time use of the cash card and calling card. The VISA cash card was depleted within a week. Even after the original source computer was shut off, the file continued to be shared by others users on P2P file sharing networks.

Professor Eric Johnson from Dartmouth will explain this test in more detail in later testimony to this committee.

Corporate Information Test

A similar Dartmouth experiment was conducted with documents related to a fictitious company placed on a Dartmouth test computer and shared using LimeWire file sharing software. Tiversa then tracked the spread of these files from the original source computer across P2P networks clearly indicating that there was significant "demand" for these "corporate" files.

The Root of the Problem

Why is there such a pervasive and massive amount of sensitive, classified, and confidential information available on peer-to-peer file sharing networks? Corporations and government agencies have installed technologies designed to block access to P2P networks and instituted policies that prohibit employees from using P2P networks or taking or e-mailing information to their homes. Consumers have installed virus checking and firewalls, which is typically the recommended course of action by the world's major security software providers.

Tiversa's focus has been working with corporations, government agencies, and consumers to mitigate P2P disclosures and risks. Based on our experience, we believe the reason so much information is present is driven by these factors:

1. A lack of awareness to the pervasiveness and magnitude of sensitive and classified information present on P2P networks. One cannot "fix" a problem that one is unaware of, no matter how much it currently may affect an organization.

2. Overextended information security functions and budgets that prioritize recent "fires" or compliance with legislation and industry mandates. Prioritizing something to which there is little awareness is often not done because it is difficult to gain the attention of senior management and procure budgets and resources.

3. Organizations have "too narrow" a view of their network perimeter. Whose responsibility is it to protect information once it leaves the corporate perimeter? Does a consumer or the US government care

whether a corporation or a supplier to that corporation entrusted with sensitive information disclosed files on P2P File Sharing Networks once the damage is done? The overwhelming evidence shows that a substantial amount of P2P inadvertent file sharing breaches come from an organization's *Extended Enterprise* outside of its network perimeter. Many organizations today focus solely on protecting their network perimeters when their business is becoming more virtual and outsourcing is taking hold. Sensitive, confidential, and classified information follows these new business operations.

Finding Solutions

We would like to provide the committee our initial recommendations on how consumers, corporations, and government entities can mitigate this problem.

The committee should take steps to:

- Create broader and more focused awareness of the dangers of inadvertent P2P file sharing.
- Require continuous auditing of P2P file sharing networks themselves for sensitive, confidential, and classified information disclosures.
- Encourage organizations to adopt policies and to take steps to address their *Extended Enterprise.*

Consumers:

For consumers, Tiversa has a number of recommended actions

- Consumers first need to become aware of this problem. While government warnings already exist, we feel the private sector can play a highly effective role in addressing this issue and in creating awareness. Banks, credit card companies, and healthcare insurance organizations can lead this effort since they are most impacted by P2P originated fraud. They are trusted by their customers and have existing communication channels available. Previous efforts to address phishing serve as a useful model.
- Consumers should consider putting their highly sensitive information on a separate PC or device disconnected from the Internet.
- Consumers should continuously audit P2P networks to ensure that unwanted files are not exposed. If they find personal or sensitive information available, they should be equipped with the knowledge of what actions to immediately take.

Corporate

For corporations, Tiversa has a number of recommended actions:

- Those tasked with managing security risks inside of an organization must be aware of the pervasiveness and magnitude of inadvertent P2P file sharing, and how it affects them. These individuals need to educate senior leadership – especially those in privacy, legal, and compliance – to the risks they face.

- Corporations need to understand their disclosed information exposure by auditing, as fully as possible by a neutral third party, the type and magnitude of their information on P2P file sharing networks.

- Corporations need to continuously monitor for new exposure points on P2P networks, and to judge the effectiveness of their policies and remedial actions.

- Corporations need to identify disclosure sources across their Extended Enterprises that expose them to inadvertent file sharing risks. This includes employees operating outside of the perimeter, suppliers and contractors, agents, and partners.

- Corporations should re-evaluate "four-wall" perimeter approaches to information security and update their policies to address information disclosure by third parties and the general lack of control once information exits an organization. This may include, for instance, requiring contractors, suppliers, attorneys, and accountants to indemnify the organization for peer-to-peer originated information disclosures.

Government

- The government should take the lead in creating greater awareness at corporations and throughout the public on the dangers associated with P2P file sharing.

- The government should immediately and continuously identify the full exposure and global spread of classified information to shut down these disclosure sources.

- The government should conduct a comprehensive audit of P2P file sharing network information disclosures – not just focused on the agencies themselves, but on also on contractors and non-agency sources.

- P2P information exposure risk should be emphasized in the Federal Information Security Management Act Report Card.

- The government should require their contractors to certify that they and their extended enterprises have fully addressed inadvertent file sharing disclosure risk.

Conclusion

In conclusion, the inadvertent file sharing through P2P File Sharing networks is highly pervasive and large in magnitude. It affects consumers, corporations of all sizes, and government agencies.

Existing policies and IT measures have not been effective at preventing information from becoming available. Malicious individuals regularly use P2P file sharing networks to obtain sensitive, confidential, or classified information. They pose an immediate threat to national security, business operations and brands, and consumer fraud and ID theft.

The committee should seek to create broader awareness of the problem. It should encourage individuals, corporations, and government agencies to continuously audit P2P networks themselves to enable these entities to intelligently determine their exposure and to design strategies to mitigate their issues.

Mr. Chairman, taking these steps will better protect us all from the dangers that lurk in these networks while allowing for legitimate uses of the technology in the future.

Thank you for the opportunity to testify here today.