Testimony of Vincent Gullotto
Vice President
Anti-Virus Emergency Response Team (AVERT)
Network Associates, Inc.

Before the
House Committee on Government Reform
Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census

"Worm and Virus Defense: How Can We Protect the Nation's Computers From These Threats"

September 10, 2003

Chairman Putnam, Ranking Member Clay and Members of the Subcommittee, I want to thank you for inviting me to testify today on the important topic of protecting our nation's computers from the threats of viruses and worms. My name is Vincent Gullotto, and I am Vice President of the Anti-Virus Emergency Response Team (AVERT) at Network Associates, Inc. I am honored to be invited to be here today to join my distinguished colleagues from government and industry alike to discuss with this Subcommittee the current state of virus and worm attacks on our nation's computers, systems, networks and infrastructures. I also look forward to making recommendations for how we can protect ourselves from these rapidly increasing threats.

With headquarters in Santa Clara, California, Network Associates, Inc. is a leading provider of intrusion prevention solutions for network and systems security. Network Associates is comprised of three product groups: McAfee Security, which offers desktop and network anti-virus and security products; Sniffer Technologies, which provides network availability and network protection; and Magic Solutions, which develops service management solutions. In addition, we are home to Network Associates Laboratories, widely recognized as a world leader in information security research and development. Our customers range from the largest of enterprises, universities and governments, to medium and small businesses, to millions of consumers around the globe.

Network Associates is committed to working with consumers, business, academia and government to identify emerging cyber threats, risks and vulnerabilities, and to develop solutions that can be distributed rapidly and widely. As a company, we participate in a number of collaborative organizations. We are Founding Members of the Partnership for Critical Infrastructure Security, the Online Identity Theft Coalition, the Organization for Internet Safety and the National Cyber Security Alliance's Stay Safe Online campaign. We co-chair the Department of Commerce's International Outreach Subcommittee of the Communications and Information Sector Working Group. And we actively participate in the cyber-security efforts of a number of trade associations, including the Business Software Alliance, the Information Technology Association of America, the Alliance for Network Security and the Security Research Alliance. Each of these entities is devoted to building partnerships between government and industry to improve the way we prevent, identify, respond to and recover from cyber attack.

I am here today to share with you my perspectives as head of the Anti-Virus Emergency Response Team (AVERT), the anti-virus research arm of Network Associates. Located in 18 cities worldwide, AVERT is responsible for the research and discovery of computer viruses, including Melissa, LoveLetter and Bubbleboy, the first virus written that could infect a user by simply previewing an e-mail. The AVERT group is also credited with the discovery of the first wireless virus, Phage. Like its name implies, the Anti-Virus Emergency Response Team serves as a front-line in the fight against viruses and worms.

In order to fight the constantly evolving threats, AVERT cooperates with our colleagues in the anti-virus field. Three years ago, ten leading anti-virus researchers, including three from AVERT, created the Anti-Virus Emergency Discussion Network (AVED; http://www.aved.net) as an effort to thwart the rapidly spreading viruses. There are now 64 participants in this organization from 27 different anti-virus companies around the world. As you can imagine, this spirit of cooperation plays a significant role in protecting all of us from the threats from viruses, worms and other attacks.

In addition to AVERT's work with customers, partners and other researchers, we are committed to working closely with law enforcement, security and intelligence organizations to assist in their efforts to fight cybercrime worldwide. Stopping viruses and worms at their source by identifying and prosecuting their authors is a key part of our mission to help solve the computer virus problem.

Overview

Mr. Chairman, I'd like to commend you and the Members of this Subcommittee for your leadership in holding today's hearing. As the last few weeks have shown us, the impact of viruses and worms on our computer systems is rising dramatically. The computer virus infection rate has grown to speeds never before seen. And the damage caused by such attacks is escalating.

As the recent electricity blackouts in the northeastern part of the United States have shown, we as a nation are more interconnected than ever before. Our electrical systems, our telecommunications, our information technology, our financial services, our transportation and our emergency services all rely upon each other to operate effectively, and a hiccup in one can cause significant cascading effects on the others.

As we examine how to protect ourselves against malicious cyber-attacks, such as worms and viruses, it is important to view the issue not simply as an effort to avoid the annoyance of a flood of e-mails or a crashed system. The challenge must be viewed in the broader context of the potential vulnerability of our critical infrastructures. During the Slammer virus outbreak, major U.S. banks experienced widespread ATM outages, a major airline canceled or delayed flights, and a large U.S. metropolitan area lost its 911 emergency services. As a result of the more recent outbreaks, a major airline lost the use of its computer system for reservations and check-in, already cash-strapped state and municipal governments wasted numerous resources to address their network problems, and colleges and universities faced the risk of students bringing virus infected computers to school and crashing or slowing down the school's network infrastructure.

The threats are real, and the consequences of inaction or insufficient action are significant. But this is not a doomsday scenario. Attacks such as those that occurred over the last several weeks provide an important wake up call to governments, industries, and consumers. We must not be complacent; we must act. To ensure the stable, efficient and predictable operations of our critical infrastructure, we must consistently try to stay one

step ahead of the attackers, and we must implement technologies to proactively protect our systems rather than simply react as the damage is being done. The technological sophistication of the attacks may be growing, but so is the technological sophistication of the solutions. We will continue to innovate to stay one step ahead.

Viruses and Worms: Definitions and History

Before describing steps we can take to protect ourselves from worms, viruses and other attacks, I believe it would be helpful to provide a short background on the history and development of viruses and worms. With this background, I will present a series of trends that bring us to today's (and tomorrow's) security challenge.

The common belief is that anything bad happening on a computer is caused by a virus. Not so. Viruses are programs that spread. A traditional virus spreads by jumping from program to program. Worms, a term recently in vogue, generally spread from machine to machine. But a worm is a type of virus. Separately, a Trojan—as its name might imply—acts in ways that the user would not expect, but the author intended.

Deliberate exploitation of security vulnerabilities in software is increasingly common and plays a large role in recent virus and worm activity. Automated worms that spread without human interaction will usually involve such an exploit. Personal firewalls can be used to hide exploitable software from being vulnerable to the Internet. Anti-virus and intrusion prevention software can block many of the known exploits. But to really eliminate the possibility that a vulnerability will be exploited, one has to update to the latest version of the deficient software.

For most of us, paying attention to information security started out of necessity, to combat a nuisance. To see how that has changed, let me give a brief history of viruses.

Pre-1995: Boot and Com Infectors (Small-Scale Damage)

Until 1994 or earlier, viruses like Michelangelo, Brain and FORM were spread by floppy disks being passed from user to user, and were relatively easy to stop. IT staff usually had weeks or even months between the time a new virus was discovered and when it might show up on the network.

The cost of these viruses was minimal, as they were mostly produced manually as proofs of concept to expose a vulnerability while showing some proficiency of programming. The number of people who could do it, and had the motivation to do it, was fairly small.

1995 to 1998: Macro Viruses (Large-Scale Nuisance)

From 1995 to 1998, the most prevalent viruses were macro viruses, the most common being the Word macro virus. Viruses like Concept, Cap and Laroux exploited scripting languages in common applications, and were spread by users working on the same file. We started to see more costs associated with these viruses, both because of their scale and

because there were more destructive viruses being written. The justification for this was sometimes given as activism against large companies by virus writers who suggested that any kind of homogeneity bred a lack of computer security.

1999-2000: Mass Mailers (Servers Clogged by a Double Click)

In 1999, we saw the rapid rise of the e-mail-aware virus in which servers could be clogged by a double click. The first was Melissa, which hit on Friday, March 26, 1999. We have continued to see minor variations on this theme for the past couple of years, including viruses like Loveletter (i.e., the Love Bug), and a virus named after Anna Kournikova. Each of these mass mailer viruses used Visual Basic script to read the user's address book and then e-mail copies of itself to other users, who then opened the e-mail because it came from someone they knew.

This new method meant viruses started spreading more quickly than ever before. The network downtime associated with these viruses and others like them made them much more costly—at $29 billion, almost three times as expensive as the past four years and in half the time.

A variation of this type of mass mailing threat, the Bubbleboy virus, was discovered by AVERT in November 1999. In this variation, a user did not need to "click" an attachment to get infected, as the virus would launch upon the user simply opening the message itself.

2001 to Present: Worms (No User Required)

All of this was a precursor—a training ground, if you will—for the kind of threats we saw in 2001, when we began to see a new kind of virus writer and a new kind of virus: the Internet worm. Internet worms don't require a user action to spread. Once let loose, they crawl through known holes to infect new systems as fast as they can. Code Red and Nimda are two of the most severe worms to date, but our McAfee AVERT researchers have seen hundreds of examples of these worms since that time. Most significantly, with these attacks the Internet shifted from being a method for distribution to a target itself, as we saw when Code Red slowed Internet traffic by as much as a third around the globe.

Because there is no user to act as a gating factor to stop the spread of an Internet worm, the reaction time for individuals, companies or governments to protect their network has narrowed to minutes. This new threat fundamentally changed the nature of the required response to virus threats. And in response, we need to rethink the way we fight them.

Today and Tomorrow – The Compound/Unified or Blended Threat

Today, and in the months and years ahead, we face a compound/unified—or blended—threat. The term and the actual date of the first threat of this type might be argued, but what can't be argued is its ability to cause havoc.

Blended threats are designed to prey on vulnerabilities discovered in operating systems or applications. This type of attack has become prolific over the past two years, and the

threat will continue. Blended threats thrive on vulnerabilities, and there will be more vulnerabilities discovered in the months and years to come. Therefore the quest must be to find ways in which threats like CodeRed, Nimda, Klez, Slammer, and Lovsan can be stopped before they cause any damage.

Let me make one final comment on these threats and others like them. The threats listed above have many commonalities and many individual traits that have made them high impact threats throughout the past three years. They all have followed the evolution of the technology we've created to make using the Internet a faster and more convenient mode of doing business, sharing data, and communicating. Because there is common ground on which they operate, there is common ground on which we can protect each other from these and future threats.

To help understand the true workings and impact of the most well-known viruses and worms, please see **Appendix A: "Well-Known Viruses and Worms."**

Viruses and Worms: Trends

Most companies have deployed security technologies to protect their IT infrastructure. Yet, they remain vulnerable because the threats are rapidly evolving, and up until now most security technologies have been reactive rather than proactive in nature. There are several reasons why reactive response is no longer sufficient.

The speed of attacks has accelerated tremendously. Well-known "denial of service" worms like Code Red and Nimda spread around the globe in a day or less. Recently, the time required for such attacks to be felt globally has shrunk tremendously. On January 25, 2003, SQL Slammer infected over 5,000 servers around the world in UNDER THREE MINUTES. The time it takes for an attack to be created to exploit a vulnerability is shrinking. When a vulnerability is discovered in an operating system or an application, and a patch is released, it takes time to deploy the patch to vulnerable systems. Attackers exploit a "window of vulnerability" between when the vulnerability is announced, and when all affected systems can be patched. Today, the time it takes for a threat to be created to exploit a vulnerability is about three weeks. This is the time between when the vulnerability exploited by Lovsan was announced and when Lovsan itself was discovered. This timeframe is down significantly from the six months that elapsed before CodeRed took advantage of the vulnerability in Microsoft IIS. Three weeks is not a long time to prepare for something when, like many corporate information security professionals, you have the responsibility for making sure 50,000 machines are not vulnerable.

There are theories that one virus can cripple the Internet in 15 minutes. How long might it take for someone to create a multi-tiered approach that combines a mass-mailer and a DDoS (Distributed Denial of Service) attack? The future might present us with a situation

where only a few days or few hours are available for us to prepare for such an attack after a vulnerability has been announced.

Companies and governments are becoming more porous. In recent years, companies have opened their enterprises to serve their customers better and improve the productivity of employees and suppliers. They reach out to their customers to deliver service or information through web based applications. They deliver work flexibility to their employees, with wireless networks and telecommuting arrangements. And over time, we've evolved to a highly mobile, interconnected society where most professionals will have a network connection "at their fingertips" that can interact automatically with proximity networks and the corporate extranet. Enterprises are becoming electronic sponges. They are porous, and it is getting hard to tell the "inside" from the "outside."

Reported vulnerabilities are on the rise. The bad news is that the new threat—worms that exploit vulnerabilities—can cause even greater damage. One exploited hole can have major impact. In every virus wave we've seen before, we had a single application or process that was being exploited in slightly different ways – first booting from a floppy, then Word, then Outlook. In this wave of Internet-borne worms, we're seeing an explosion in activity that exploits multiple holes in multiple applications. There's no one application or process you can watch to make sure you're secure. It's about multiple layers of defense at all times.

Protecting Against Viruses and Worms: Technology and Practices

Protecting ourselves from current and new forms of threats requires both technology and improved security practices. In technology, we must look toward a new way of thinking: proactive security. In practices, we must look toward current and emerging best security practices.

Through Technology: Proactive Security

Today, IT staff is fighting a battle that appears hard to win. Attacks get in through firewalls. Systems cannot be patched fast enough to be hardened. Intrusion detection systems generate mountains of data. The result is a growing "window of vulnerability" between the appearance of a new threat and a company's ability to deploy a fix.

What's required in order to redress the balance and close the "window of vulnerability" is protection in-depth, including solutions that can be deployed before a new threat appears in the field so that the threat "bounces off" the company's defenses.

Intrusion prevention can fundamentally change the equation through precision blocking of known and unknown threats in real time. Intrusion prevention looks for anomalies and attack signatures and responds by preventing the attacks from permeating the network or system defense. An intrusion prevention system protects a network from attack, while providing breathing room and response time for analysts to fix vulnerabilities.

Intrusion prevention is about identifying threats to your business and blocking them, helping enterprises, small businesses and government agencies assure the availability and security of their desktops, application servers and web service engines.

Through Practices: Best Security Practices

In addition to technology, best security practices also play a key role in protecting ourselves from the threats of viruses, worms and other attacks. The following are a few key elements of best security practices.

First, it is important to know your critical assets. It is vital to know what they are, where they are, how critical they are to your mission, and what their vulnerabilities are.

Next, it is important to understand and assess the threats you face. What kinds of threats do you face from hackers, industrial spies or an enemy state? Where is the threat most likely to come from – Inside2Outside, Inside2Inside, or Outside2Inside? And, how severe can the impact be?

Third, it is important to know your protection needs and the defense tools–firewall, intrusion prevention, anti-virus, vulnerability assessment, access control–that help you address those needs. It is also critical to know how these tools fit in with your security strategy.

Finally, it is imperative to address the cyber threat challenges systematically. This includes:

- A layered defense with multiple methods of protection including signature based and behavioral based detection
- Integrated response to attacks
- A proactive approach that involves blocking attacks, not merely detecting them
- Well defined security policies with real enforcement

Recommendations for Action

While this testimony covers a number of areas, I respectfully would like to make a series of key recommendations. These recommendations fall into three audiences: government policymakers, enterprise users and consumer end users.

Government Policymakers

While ensuring strong cyber-security and protecting against virus and worm attacks is primarily a technology and practices issue, we believe that there is a role for government policymakers. We offer three recommendations.

1. Look to Cyber-Security Industry as "Cyber First Responders"

In Homeland Security discussions, much focus (rightfully so) is on the critical role of First Responders. We respectfully suggest that the cyber-security industry represents "Cyber First Responders" in our battle against attacks on the information infrastructure. Policymakers, in addressing the threat of viruses, worms and other attacks, should turn to these Cyber First Responders to craft public policy that embraces technology as a fundamental part of the solution. Cyber First Responders, in a collaborative partnership, can provide policymakers with real-time, non-hyped, accurate information about the nature of the threats and the extent of the impact. And in crafting potential public policy, policymakers should be cautious to do no harm to a highly innovative and responsive cyber-security industry.

2. Promote a "Culture of Security"

Policymakers and industry representatives in the U.S. and abroad have discussed the need to promote "a culture of security." We believe that policymakers around the world can embrace this concept by continuing to shine a light on cyber-security. Policymakers can support public awareness efforts (e.g., the Stay Safe Online campaign), government/industry collaborative bodies (e.g., the Partnership for Critical Infrastructure Security), focused government leadership (e.g., a high-ranking single point of command), and real-time information sharing organizations (e.g., the various vertical sector information sharing and analysis centers). Finally, policymakers can explore the business models and drivers under which industry operates. Where there are gaps between national infrastructure needs and business drivers for action, policymakers can explore "carrot" and "stick" (or incentive and requirement) approaches for industry to take action.

3. Support Cyber-Security Research & Development

In addressing our cyber-security challenges, research and development plays a key role in allowing us to stay ahead of the next generation of attacks. Yet, many of the R&D challenges go beyond ROI formulations for individual companies. Government has played and will continue to play a critical role in supporting longer-term R&D. In the area of R&D, we recommend that policymakers:

- Authorize a study of our nation's critical infrastructure vulnerabilities
- Increase R&D funds to leading departments and agencies (e.g., NIST, DARPA, HSARPA, NSA, NSF and others) for collaborative R&D with industry and academia
- Refocus collaborative R&D on longer-term challenges, realizing that true ROI may not occur until years 3 or later of a project
- Improve coordination among government-funded R&D projects

Enterprise Users (Commercial, Government and Education)

Enterprise users, whether large corporations, small or medium-sized businesses, government agencies or educational institutions, often experience the brunt of the attack from worms and viruses. While policymakers can develop an environment supportive of strong cyber-security, enterprise users can take steps to minimize risks and block attacks. We offer two recommendations.

1. Implement a Proactive Security Strategy

As discussed earlier, the traditional approach to cyber-security has been a reactive strategy, through updating virus definition files and detecting when attacks take place. Technology has evolved and now allows enterprise users to become proactive. With the delta between the discovery and the subsequent exploitation of vulnerabilities shrinking dramatically, we recommend that enterprise users embrace intrusion prevention to ensure that their networks and businesses stay up and running even when they are under attack.

2. Educate Your Users

As part of an intrusion prevention strategy, enterprises should focus resources on training and educating their internal end users. Whether acting maliciously or, more often, simply being the victims of social engineering tactics, enterprise end users can often be an organization's greatest vulnerability. With mandatory, ongoing training and education classes on cyber-security, end users—executives, employees, or students—can close the "window of vulnerability."

Consumers

Finally, consumers at home also play a key role in stopping the damage caused by viruses, worms and other attacks. Often home systems, without the support of a dedicated IT department, are the most vulnerable to these attacks. To help consumers close this hole, we make two recommendations:

1. Protect Thyself

Just as we learn to take steps to protect our physical home through locking doors and windows and screening strangers, consumers at home also should take the time to learn a couple fundamentals of cyber-security. Without requiring consumers to become cyber-security experts, we should continue to provide consumers with easy-to-understand resources on how to protect themselves through anti-virus products, personal firewalls, and other technical measures. In addition, these resources should include important best practices, such as deleting or scanning attachments and recognizing suspicious e-mail messages. The Stay Safe Online website (www.staysafeonline.info) is a good start.

2. Demand Strong Cyber-Security of Others

Consumers also can play a role through their purchasing power. We recommend that consumers prioritize security features when selecting an Internet Service Provider (ISP), even if it means paying an additional fee for extra layers of security. We also recommend that consumers inquire about the cyber-security of their online transactions, whether with banks, retailers, on-line auctions, government services, health care providers or others.

While taking steps to implement the above recommendations will not ensure total protection from viruses, worms and other attacks, these actions will have a significant effect on the impact of these attacks. Policymakers, enterprise users and consumers each can play a role in protecting ourselves and our infrastructures from cyber attack.

Conclusion

Mr. Chairman, the challenge before us today is significant. The speed of cyber attacks has accelerated dramatically. Companies and governments have become more porous. Reported vulnerabilities are on the rise. And vulnerabilities are being exploited more frequently and faster. In order to fight the challenges of tomorrow, we must not rely on the tools of today.

But there are steps we can take to make a real difference. Policymakers can embrace Cyber First Responders, support a culture of security and support critical long-term research and development. Enterprises can shift toward proactive security through intrusion prevention while educating their users in security essentials. And consumers can learn security fundamentals and demand them of those with whom they do business.

As we commonly know in the industry, security is a journey, not a destination. We urge your Subcommittee and Congress to continue putting energy into addressing the cyber-security challenge. In return, I pledge to you our company's support to continue to work with government, industry and academia to develop solutions to these urgent needs. I repeat what I said earlier, the technological sophistication of the attacks may be growing, but so is the technological sophistication of the solutions. We will continue to innovate to stay one step ahead.

I thank you again for the opportunity to testify here today, and I look forward to answering any questions the Subcommittee may have.

Appendix A: Well-Known Viruses and Worms

LoveLetter

The LoveLetter virus is noted as the most costly virus incident ever. It was the first of its kind and the most widely distributed virus making use of the .VBS extension. Much of the cost attributed to this virus is due to the virus's effect of overwriting all files bearing the extensions .vbs, .vbe, .js, .jse, .css, .wsh, .sct, .hta, .jpg, .jpeg, .mp2, and .mp3.

The virus initially arrived as an e-mail with the following characteristics:

Subject: **ILOVEYOU**
Message: **kindly check the attached LOVELETTER coming from me.**
File attachment: **LOVE-LETTER-FOR-YOU.TXT.vbs**

Who could resist opening such an e-mail that played with the hearts and emotions of all? This virus is probably one of the best socially engineered viruses ever released. Social engineering, or the ability for one to craft a virus so that most anyone will open it, has become almost an art in some respects. Some social engineering messages work and some don't; a lot of the success comes down to timing and just the right amount of curiosity. The most impacted were small businesses, unable to maintain the proper backups and heavily dependent on their website operations. The combination of the wide spread of the virus and damage to files that were not backed up accounts for the exorbitant damage figure of over $8 billion worldwide.

CodeRed

CodeRed was a perfect example of a worm. It was also what is known as a file-less virus. There was nothing to click or grab on to. Thus, it moved through the Internet with relative ease, as there was almost nothing from a security software perspective that could stop it. CodeRed travels using the same networking protocol and port as normal Web traffic and took advantage of an existing vulnerability in Microsoft IIS (Internet Information Server) application both versions 4 and 5. Thus the solution to this problem was as simple as fetching the patch available from Microsoft (http://www.microsoft.com/technet/security/bulletin/MS01-044.asp) or any subsequent cumulative patch.

The damage attributed to CodeRed is much less than that of LoveLetter. Part of this is because some of the machines were subsequently taken over by Nimda, to which the cleanup cost was attributed.

Nimda

Nimda is a blended threat. It makes use of at least five different attack modes, including backdoors left by previous viruses. Coming close on the heels of other viruses, without much time for its development, we believe Nimda was created by a team of people, not just a solitary virus coder. But what Nimda demonstrated is that if we don't protect

ourselves, our own machines could be universally commandeered and used against us in a matter of hours or minutes.

An estimated quarter million to a half million machines were overcome by the virus. And many of those machines were well-known websites or mail servers for medium to large companies. In total, over 50,000 important Internet sites were infected.

SQL Slammer

Slammer is another perfect example of a worm. It exploited a vulnerability in the SQL Server Databases. This threat was responsible for knocking out ATMs and other important websites around the world that use the SQL technology. This threat —while significant—only targeted servers and did not have a major impact on Internet traffic. It did not hit home users' systems or most corporate desktops. So while its costs were high, a major portion of the machines that use the Internet were spared...at least for the time being.

SoBig

The recent SoBig virus has been the most prolific virus to date. The virus is responsible for spreading upwards of half a billion e-mail messages on the Internet. SoBig is similar to all of the other mass-mailing e-mail viruses, though it forges the sender address on its e-mails. As a result, the virus fools victims into believing it might have come from someone they know. By making it hard for friends to contact the infected party, the virus is able to reside on systems until it reaches its built-in self-termination date.

Lovsan (a.k.a Blaster)

Part of the major impact of the Blaster worm was its focus on home users. The worm attacked a port that is generally not useful to the average home user. While the impact of the worm is significant, the truly alarming lesson learned is the dramatically shortened timeframe we saw between the announcement of the vulnerability and the successful release of a worm targeting that vulnerability. How can we prevent such attacks like Blaster? A default setting that does not allow traffic on similar ports would inhibit such attacks.

Appendix B: Biography

VINCENT GULLOTTO
Vice President
AVERT (Anti-Virus Emergency Response Team)
Network Associates, Inc.

Vincent "Vinny" Gullotto is the vice president of research for AVERT (Anti-Virus Emergency Response Team), the anti-virus research arm of Network Associates. For roughly half a decade, Vinny has been intimately involved in the day-to-day operations of AVERT Labs.

Located throughout 18 cities worldwide, AVERT Labs is responsible for the research and discovery of computer viruses, including Melissa, LoveLetter, Bubbleboy, the first virus written that can infect a user by actively opening an attachment in e-mail. Under his leadership, the AVERT group is also credited with the discovery of the first wireless virus, Phage.

Vinny's creation of the AVERT research group was driven by a business model that puts customer service first. The model allows his group to focus on having the best virus detection rates in the industry. His involvement includes the design and development of McAfee's anti-virus scanning engine and virus detection technology, working round-the-clock to maintain and manage AVERT's global research capabilities.

He also works on an ongoing basis with other global members of the anti-virus community in detecting viruses. Vinny has developed the concepts and initial designs for a number of AVERT service and solution offerings. They include programs such as WebImmune (www.webimmune.net), the world's first Internet virus security scanner that resides on the Web; as well as the AVERT Malware Stinger, a stand-alone program designed to supplement anti-virus programs by going beyond traditional technology available today, serving as a test bed for components to be included in Network Associates' McAfee VirusScan engine.

When it comes to virus research and virus outbreaks, Vincent Gullotto plays an integral role in advising and alerting the public through various outlets, further enabling the public to take necessary precautions to protect themselves.

Vinny can be found giving insight regularly in technology trade publications and on technology centric Web sites. He has been instrumental in providing insight and perspective about virus events such as Melissa, LoveLetter, and CodeRed on major news networks that include CNN, ABC World News, CBS, ZD Net, CNET and IDG.

Vinny has spoken around the world, serving as a primary spokesperson for Network Associates and AVERT at press conferences, sales conferences, customer and non-customer conferences. He has also shared his vast knowledge of the anti-virus field by presenting at several security conferences, including COMDEX, Networld+Interop, the E-Security Expo , Sector 5 Security Conference and the SANS Institute conference.

Additionally, Vinny has addressed and directed a session at EICAR (European Institute for Computer Anti Virus Research), covering e-commerce and security risks associated with purchased made on the Internet.

He recently spoke at the CampIT Expo in Chicago and at the Forum ICT Conference in Rome Italy where he addressed today's threats, where they evolved from and what may be seen in the future.

Prior to AVERT, Vinny held a director and Board of Director's position at a privately held US firm that pioneered and developed cost-efficient, PC-based automated attended voice mail systems. Vinny holds a Bachelor of Science degree in Business Administration from the University of Phoenix.

Appendix C: Disclosure of Sources of Government Funding

September 8, 2003

The Honorable Adam Putnam
Chairman, Subcommittee on Technology, Information Policy,
Intergovernmental Relations and the Census
House of Representatives
B349-A Rayburn House Office Building
Washington, DC 20515

Chairman Putnam:

This letter serves as financial disclosure in accordance with the rules of the House of Representatives governing non-government witnesses and federal grants and contracts. I submit this disclosure in advance of my appearance before the Subcommittee on September 10, as a witness for the Subcommittee's hearing on computer viruses and worms.

The products and services of Network Associates, Inc., including McAfee Security, Sniffer Technologies and Magic Solutions, are used extensively throughout the Federal government. Network Associates has contracts with defense and civilian departments and agencies alike, including but not limited to the Departments of Defense, State, Justice, Treasury, Interior, Health and Human Services and Education as well as many independent agencies, commissions and administrations.

In addition, Network Associates Laboratories conducts federally-funded advanced security research for the following organizations:

- Defense Advanced Research Projects Agency (DARPA)
- National Science Foundation (NSF)
- National Institute of Standards and Technology (NIST)
- Army Research Labs (ARL)
- Air Force Research Labs (AFRL)
- Advanced Research & Development Activity (ARDA)

If you or a member of your staff has any questions about these sources of funding, please feel free to contact me.

Sincerely,

Vincent Gullotto
Vice President, AVERT
Network Associates, Inc.