Computer & Communications
Industry Association

666 Eleventh Street, N.W., Sixth Floor
Washington, D.C. 20001
202.783.0070 Fax 202.783.0534

August 27, 2003

The Honorable Tom Ridge
Secretary
U.S. Department of Homeland Security
Washington, D.C. 20528

Dear Secretary Ridge:

In light of last week's events revealing additional serious flaws in the Windows software bundle, I am writing concerning the Department of Homeland Security's choice of Microsoft as the preferred supplier of desktop and server software for its computing needs. I strongly urge you to reconsider this decision.

The Computer & Communications Industry Association (CCIA) is an association of computer, communications, Internet and technology companies that range from small entrepreneurial firms to some of the largest members of the industry. CCIA was founded over 30 years ago and our members include equipment manufacturers, software developers, providers of electronic commerce, networking, telecommunications and online services, resellers, systems integrators, and third-party vendors. Our member companies employ nearly one million people and generate annual revenues exceeding $200 billion. Although we have always supported open, industry-wide fair and efficient procurement policies, we do not represent companies in the bidding and procurement process.

CCIA also has a long history of advocacy and expertise in the area of cybersecurity. We recently pointed out in submissions sent to the Administration and the Congress the importance of security testing, the dangers of relying on single suppliers for information technology, the inherent risks associated with homogenous systems, and the need for "biodiversity" among software components and applications.

We believe that for software to be truly secure it must be well written from the outset with security considerations given a high priority. Unfortunately, there is ample evidence that for many years economic, marketing, and even anticompetitive goals were far more important considerations than security for Microsoft's software developers, and these broader objectives were often achieved at the cost of adequate security. Also, from a security standpoint, the lack of diversity within a networked system amplifies the risk emanating from any vulnerabilities that do exist. But diversity is difficult without interoperability, and the benefits of interoperating with more robust systems can be blocked if any dominant player does not cooperate in fostering interoperability. Unfortunately, numerous courts and government enforcement bodies, including the United States Department of Justice, have formally found that Microsoft has used technical barriers to inhibit interoperability with, and competition from, other software platforms and applications.

We are currently engaged in extensive security research in this area and our preliminary findings indicate the severity of the security problems relating to some Microsoft software is substantial. The news from the last few weeks demonstrates that this problem is not just theoretical, but real and immediate and one that imperils homeland security.

In just the last two weeks, Microsoft products have been attacked by a virus and worm -- Sobig.F and Blaster -- but these are only the most recent examples of major security failure created by vulnerabilities in Microsoft's dominant software portfolio. The damage caused by these attacks is significant and has caused millions of dollars of harm to our economy, but security experts agree the damage could easily have been much worse. According to the Washington Post, Blaster and its associated counter-measures were responsible for the temporary closure of Maryland's Department of Motor Vehicles offices, failure of the passenger check-in system at Air Canada, an intrusion on the Navy-Marine intranet, and cancellations and suspensions of service on the CSX railroad. Of even greater concern are recent reports of an April e-mail to the Nuclear Regulatory Commission from FirstEnergy detailing how a previous worm directed at Microsoft servers, Slammer, disabled a safety monitoring system at an offline nuclear power plant for close to five hours. Fortunately, the plant was not operational during the failure, there was no safety hazard, but this incident could have just as easily occurred with an online plant. All of these failures are unfortunately predictable and we can expect to continue to see similar problems in the future.

In short, we have seen these most recent worms and viruses directed at Microsoft slow down, delay, and disable systems handling critical transportation, military and energy functions. Though certainly the creator of these malicious attacks must bear the brunt of blame, Microsoft is also largely responsible for continuing to create software riddled with obvious and easily exploited vulnerabilities. This problem is compounded when new or separate products and functionalities are intricately bundled, sometimes illegally, into Windows. As the Washington Post editorialized:

> [T]he main cause of virus prevalence, say computer experts, is poorly designed software. The Blaster worm was created to take advantage of a vulnerability in Microsoft's operating system, particularly targeting Windows XP, Windows 2000, Windows NT, and Windows Server 2003. Such vulnerabilities exist because software is distributed without appropriate amounts of testing and because software vendors increasingly create new functionalities that invite infection[.]

Because of these recent developments, historical experience, and the inherent risks associated with lack of diversity, we ask that you reconsider your heavy reliance upon a single, flawed software platform to protect our national security. The latest round of worms has shown in dramatic fashion the economic damage and danger to our safety that can occur because of reliance on a single vendor who has failed to demonstrate a core commitment to security. Our hope is that you fully consider these critical concerns when implementing security and information technology in the Department.

Sincerely,

E J Black

Ed Black
President & CEO