OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE
Washington, DC 20511

The following Op-Ed by Melissa Hathaway, Cyber Coordination Executive for the Office of the Director of National Intelligence, was published by the McClatchy-Tribune News Service on Wednesday, October 8, 2008:

Safeguarding our cyber borders

By Melissa Hathaway – Op-Ed – McClatchy-Tribune News Service

London shoppers who bought groceries with bankcards over the last two years paid a higher price than they bargained for.

Cyber thieves had implanted unauthorized circuitry in keypads sold to supermarkets in the Barking and Dagenham area of the British capital. The corrupted keypads were then used to capture account information and Personal Identification Numbers (PINs). The data were siphoned off and used to skim from or in some cases empty shoppers' bank accounts.

The thieves covered their tracks by encrypting the numbers they stole, then storing them on a computer server abroad. It took more than a year for the authorities to catch on.

Stories such as that aren't only sobering news for consumers. For folks charged with securing and protecting the nation's defense and intelligence infrastructure, however, increasingly sophisticated cyber assaults are a chilling -- and increasingly familiar -- challenge.

The same devices that thieves use to sneak into bank accounts, the same techniques that hackers use to disrupt Internet service or alter a digital profile, are being used by foreign military and spy services to besiege information systems that are vital to our nation's defense.

Because defense and other national security contractors share data and systems with their government partners, an attack on one can be an attack on many. Plans are only as secure as the weakest link in the information chain. These days, those links are being tested as never before.

The attackers' goals fall into three categories:

• **Information theft.** Stealing data from a target personal device, system or network is the most common threat. For example, a disgruntled Boeing employee was charged last year with lifting more than 320,000 sensitive company files by using a thumb drive to tap the corporate system. Boeing estimated that the stolen documents would have cost it between $5 billion and $15 billion in lost revenue had they been given to competitors.

• **Information disruption.** Hackers who sneak into government systems and alter crucial operating data are a growing concern. In 2006, a disgruntled Navy contractor inserted malicious code into five computers at the Navy's European Planning and Operations Command in Naples, Italy. Two computers were rendered inoperable when the program was executed. Had the other three computers been knocked offline, the network that tracks U.S. and NATO ships in the Mediterranean Sea and helps prevent military and commercial vessels from colliding would have been shut down.

• **Information denial.** Cases in which private or government computer systems are shut down by floods of automated hits are also on the rise. In April 2007, Russian nationalists used such a "distributed denial of service" attack to block access to the networks of the Estonian parliament, the president's office and many of that country's banks, news organizations and Internet service providers.

The "What Ifs" are an even greater concern. Could an adversary insert erroneous data that would cause weapons, early warning systems and other elements of national security to fail at critical times? What if financial or medical records were altered, or rail or air traffic control systems were corrupted? What if malicious code were secretly installed during the manufacture or shipping of computer equipment, to be activated at some future date? How would we even know what threats we face?

Defensive measures are being taken. In January, President Bush proposed a 12-point Comprehensive National Cybersecurity Initiative whose solutions range from a public awareness campaign to sophisticated new systems for identifying and deterring intrusions. Congress approved funding in late September.

A key element of the plan -- reducing the number of access points between federal agencies and external computer networks -- is under way. The federal government has closed about 3,500 such access points this year, leaving about 1,000 still open. The goal is to reduce the final number to fewer than 100.

Much more needs to be done, however.

We need stronger international alliances to share the responsibility for securing cyberspace. We must do more to convince our allies and strategic partners of the benefits to them of taking an active role.

We also need a fundamental re-thinking of our government's traditional relationship with the private sector. A high percentage of our critical information infrastructure is privately owned, and industry needs to know what government knows about our adversaries' targets and, to the extent we understand them, their methods of operation.

When it comes to cyber security, government and the private sector need to recognize that an individual vulnerability is a common weakness.

There's time, though not unlimited time, to get the job done. We must make a continuing public commitment to securing cyber space -- and we must do so now.

Melissa Hathaway is the cyber coordination executive for the director of national intelligence. The Department of Homeland Security has designated October National Cyber Security Awareness Month.