

**COMMITTEE ON GOVERNMENT REFORM
SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,
INTERGOVERNMENTAL RELATIONS AND THE CENSUS
CONGRESSMAN ADAM PUTNAM, CHAIRMAN**



NEWS RELEASE

**For Immediate Release
September 22, 2004**

**Contact: Bob Dix
(202) 225-6751**

Putnam Issues National Cyber Security Call to Action

*Urges Government, Businesses and Home Users Need to Take
Immediate Steps*

WASHINGTON, DC – At a Congressional oversight hearing today examining the growing issue of identity theft, Congressman Adam Putnam (FL-12), Chairman of the House Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, called on all Americans to take immediate action to improve the overall cyber security protection of the nation.

“Today, I call on everyone in this nation to take immediate action to increase your protection and to dramatically improve the cyber security profile of this nation,” said Putnam. “We are all stakeholders, and we all have a responsibility to be part of the solution, not a continuing part of the problem.”

With the dangerous threat climate in the world today, and with the acknowledgement of widespread computer vulnerabilities confirmed by the impact of various worms, viruses, spam, backdoors, Trojans, “phishing” and spyware, there is clear evidence that national security and economic stability are at risk from attack in the cyber world.

As growth in use and access to the Internet continues to expand, and more and more information is being converted to digital form and gathered, stored and shared utilizing the Internet, there must be a renewed commitment to securing computer networks and protecting the information assets they contain

“Identity theft is one of the fastest growing crimes in the United States and it appears that the battleground is expanding from one populated primarily by those seeking notoriety to those seeking profit and disruptive impact,” concluded Putnam. “Federal

statistics show that nearly 10 million identities were stolen in the United States last year, and the total cost of this crime in the United States is approximately \$50 billion dollars a year.”

The National Cyber Security Alliance is sponsoring National Cyber Security Awareness Month during October and consumers may access information about the steps that can be taken to protect themselves by visiting www.staysafeonline.info.

Chairman Putnam has conducted 11 separate oversight hearings during the 108th Congress dealing with cyber security issues and the threat that computer and network vulnerabilities present to the national security and economic stability of this nation. The proliferation of identity theft that has been perpetrated on the American people in recent years is a manifestation of the abilities of hackers, criminals and even terrorists, to penetrate the weak defenses of cyber security.

Chairman Putnam concluded with a call to action to consumers, industry and government:

- “I call on major corporations to schedule on the agenda of your next senior management meeting and your next Board of Directors meeting, a discussion about your company’s computer information security plan. This is a management, governance and business process issue and must be treated accordingly.”
- “I call on the larger businesses of corporate America to work with your entire supply chain to demand that all of the businesses connected to your network understand their responsibility to make sure that their systems are secure.”
- “I call on the financial services sector, credit card companies, health care providers, and others to re-examine their own information security protection profiles. Many Americans trust you with their personal information and have an expectation that the information will remain confidential and protected. Why are we experiencing such a proliferation of identity theft?”
- “I call on software and hardware manufacturers and the national associations that represent them to take the lead in improving the quality and security of their products.
- “I call on Internet Service Providers and Operating Systems manufacturers to work more aggressively with other public and private stakeholders to provide consumers of all levels of sophistication with information about affordable and user-friendly tools that are available to help them protect themselves and immediately improve their cyber security hygiene.

- “I call on all small business owners to take the time and learn about steps that you can take that are affordable and user-friendly to make their systems more secure from the growing threats of cyber space. There are fundamental steps in cyber security hygiene that will improve their protection profile overnight. They are important stakeholders in this matter and have a responsibility to contribute to the solution.
- “I call on home users to become more aware of the tools that are available to improve on the protection of your home computer. Consumers must be sure to know about anti-virus software, personal firewalls, and how to update applications, including operating systems, in a timely manner.
- “I call on all states and local governments to examine their own information security plans, along with their education, awareness and training programs. Additionally, I again call on the agencies of the federal government to step up and provide the example for the rest of this nation. Receiving “D’s” and “F’s” on scorecards about their compliance with the requirements of the law is completely unacceptable. Federal CIO’s and CISO’s must be empowered to develop and implement effective strategies and to examine opportunities for enterprise solutions.
- Finally, I call on Congress to work with all stakeholders, including military, intelligence and law enforcement agencies, domestic and international, to ensure an adequate level of preparedness to meet this growing cyber challenge and to recognize this battle front in the overall threat domain.”

###