

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



**NEWS RELEASE**

**For Immediate Release  
April 6, 2003**

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

**Putnam Announces Recommendations from  
Corporate Information Security Working Group**

**Washington, D.C.** – Rep. Adam Putnam (R-FL), Chairman, Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, issued the following statement on the recommendations of the Corporate Information Security Working Group:

“As Chairman of the House Government Reform Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, I continue to work to improve the security of computers for public sector, private sector, and home users from the threat of cyber attacks. I am also focusing on the protection of information assets that are contained within computer networks.

“The Subcommittee has conducted a number of Congressional oversight hearings during the 108<sup>th</sup> Congress directly related to the efforts of federal agencies to improve their information security, and specifically their progress and compliance with the requirements of the Federal Information Security Management Act (FISMA). Since approximately 85% of this nation’s critical infrastructure is owned or controlled by the private sector, I have worked to identify strategies that will produce meaningful improvement in the computer security of corporate America. I also recognize the need to provide additional information and tools to home users to better protect them from the significant damage that can be caused by worms and viruses, or even more malicious denial-of-service attacks perpetrated through the Internet.

“Following hearings, interviews and meetings with private sector leaders, including IT and non-IT companies, I determined that information security was not a high priority matter for much of corporate America. The issue of information security is still viewed

by many as primarily a technology issue, as opposed to a management and governance issue. Therefore, the matter is not sufficiently being reviewed or considered at the “C” level of management, Board of Directors, or ownership level in the case of small and medium sized businesses. Given the magnitude and reality of the threat, I am seeking to elevate the profile of the matter and identify a means of establishing attention and accountability throughout corporate America for the security of our nation’s computers and computer systems.

“Last Fall, I drafted the Corporate Information Security Accountability Act of 2003, legislation requiring that publicly traded companies include as part of their annual filing with the Securities and Exchange Commission a status report on their corporate information security plans, in the form of a checklist that would have to be certified by an independent third party auditor. The checklist would include elements of a basic information security plan, such as: an up-to-date inventory of critical IT assets; a risk assessment and corresponding risk management/mitigation plan; an incident response plan; and a tested business continuity plan. This methodology was selected after a review of the strategies employed to motivate private sector attention to the challenges and vulnerabilities associated with the Y2K issue, as well as a review of existing legislation such as Gramm-Leach-Bliley, Sarbanes-Oxley, and HIPPA.

“Prior to filing the draft legislation, I solicited feedback from a number of private sector individuals, companies and trade associations. Following a review of that constructive feedback, and confirming that a private sector-driven, market-based initiative was always the desired preference, I decided to postpone the introduction of my proposed draft legislation, while challenging the private sector to identify an alternative approach to dramatically improve information security throughout corporate America. I made it clear that the timeline would be short, and that the draft legislation would remain a viable option.

“In order to provide the greatest value in terms of soliciting participation in such a bold, yet critical initiative, I convened a group of 25 senior leaders from nationally recognized business organizations, as well as representatives from the academic and institutional communities, to form the Corporate Information Security Working Group (CISWG).

“The group convened and met with me on November 5, 2003 to discuss the goals, objectives and expectations for the Corporate Information Security Working Group. The schedule of succeeding meetings was as follows:

November 19, 2003	Hosted by: National Association of Manufacturers
December 17, 2003	Hosted by: U. S. Chamber of Commerce
January 14, 2004	Hosted by: The Business Roundtable
January 28, 2004	Hosted by: Center for Strategic & International Studies
February 11, 2004	Hosted by: Critical Infrastructure Protection Project George Mason University- Arlington, Va Campus Full Day Working Session

March 3, 2004

Final Meeting- Report & Recommendations to  
Chairman Putnam

“Additionally, having become aware of the organization of a National Cyber Security Summit to be held in December, 2003, with a proposed reporting deliverable of March, 2004, I was interested in receiving the value of that product as well.

“The CISWG created (5) subgroups that met independently of the full CISWG and deliberated significant areas:

Best Practices and Guiding Principles  
Incentives-Liability/Safe Harbor  
Education, Awareness and Training  
Procurement Practices  
Reporting, Information Sharing, Performance Metrics

“The intent of this effort was to achieve a consensus on a set of recommendations that could form the basis of an action plan. The work session on February 11, 2004 provided an opportunity for discussion and debate about a series of recommendations.

“At the March 3<sup>rd</sup> meeting, just three months from the formation of CSWIG, four of the subgroup Chairs presented me a series of recommendations. Those recommendations are currently being reviewed and considered. The fifth subgroup is still working and not yet completed their work.

“It is important to note that a number of the recommendations require continued work, and form the foundation for the follow up work that will proceed. Virtually every member of CISWG has indicated a strong interest in continuing this important and critical work. Additionally, while it was the effort of CISWG to achieve consensus on this set of recommendations, there was not unanimity on all of the recommendations, and some members expressed concern that there were a number of recommendations that were not fully mature and required further discussion and debate.

“The body of work that is represented in the reports and recommendations contain innovative and creative approaches, utilizing a variety of tools to achieve a private-sector driven, market-based approach to addressing corporate information security in every sector, including small, medium, and large businesses and enterprises.

“I am presently evaluating the CISWG work product, along with the work of the various working groups attached to the National Cyber Security Summit to identify similar or complimentary recommendations. I am also considering other elements that may be contained in a corporate information security action plan in lieu of legislation. The CISWG recommendations include several potential legislative initiatives, such as an amendment to the Clinger-Cohen Act that would explicitly identify information security as a component that must be evaluated in the IT investment decision-making and strategic planning for federal agencies. I have already begun the process of drafting such

an amendment and I am working on an initiative that could be pursued in the very near future.

“I would like to thank the various members of CISWG who contributed so generously of their time, resources, expertise, creativity and leadership on this issue that is so important to the American people and the U. S. economy. I look forward to continuing to work with this talented group on the important follow up work that is so appropriately acknowledged in the series of recommendations.

“As the Subcommittee continues to provide oversight of federal agencies, including an annual scorecard of progress and compliance with the requirements of FISMA, I also call on businesses of all sizes throughout America to consider the matter of information security as it relates to their business. Some businesses are clearly elements of the nation’s critical infrastructure and require a different type of risk management plan; however, every business has a responsibility to practice at least basic information security hygiene and do their part to contribute to the overall security of computers and information networks in this country. Additionally, manufacturers of software and hardware products have a responsibility to continue to consider the quality and security of products that they offer to the marketplace in response to consumer expectations on behalf of users from the most sophisticated enterprise to the most unsophisticated home user.

“The collective efforts and continued attention will produce a more secure system of networks and individual computers, thereby reducing potential vulnerabilities that could be subject to a cyber attack, and thus making America a safer place for all citizens.

“A list of the participating CISWG members, along with copies of the recommendations of the Sub-Groups is attached. The more discussion and dialogue – both pro and con – the more opportunity there will be to identify productive solutions that can produce meaningful and measurable results. The recommendations will soon be posted on the Subcommittee website at <http://reform.house.gov/TIPRC> .”

###