



A Call to Action

by: Andy Hagg

文章简介：本文首先阐述了国家关键基础设施保护（CIP）的重要性，号召与关键基础设施相关的私营机构参与到 CIP 工作中。接着本文还简单介绍了与此相关的一些文章及其讨论的议题。



[华安信达](http://ChinaCISSP.com)

America's critical infrastructures are vulnerable to attack. Technological advances have afforded us a vast network of efficient, automated systems, upon which rely the essential functions of our society. Our utilities, financial data, communication capabilities, and emergency services all operate on computer-controlled networks, which could be shut down by a 14-year-old hacker or a militant terrorist organization.



The purpose of this *Contingency Planning & Management* supplement on Critical Infrastructure Protection (CIP) is to raise awareness among the private-sector custodians of the infrastructures at risk by reporting on what the government is presently doing to protect the infrastructures, demonstrating what the private sector is doing, and most importantly suggesting what you as an executive officer or business continuity professional in a critical sector of American industry can do to protect your company and your country from attack.

The threat has been termed cyber-terrorism, cyber-warfare, cyber-attack, and information warfare. Maybe we can call it e-spionage. Whatever we choose to name it, the threat is real, and awareness must be raised. Far too few companies are doing enough to protect themselves against e-spionage, and I fear that the reason may lie in the messenger. With the President's Commission on Critical Infrastructure Protection of 1997 and the subsequent Presidential Decision Directive 63 of 1998 initiating much of the effort among government organizations to warn of the vulnerabilities of our infrastructure to cyber-terrorism, the private sector has in many cases taken a guarded stance against such proposals to work together. As you'll see in ["CIP: The History, the Hurdles Ahead"](#), there has been much debate between industry and government on jurisdictional issues, with the government claiming to just want to help and privacy advocates seriously concerned about rights that could be violated in the sharing of proprietary information with the government, particularly law enforcement officials.

Businesses hesitating to act because of this power struggle should not turn Paul Revere away because they don't like the color of his horse. They should heed the warning sounded by the likes of PDD 63, the NSC, the CIAO, and the NIPC, and do something, even if they only feel comfortable starting at home—building up their own networks' defenses, communicating with their own departments, suppliers, and partners about threats of intrusion and foul play. Eventually, though, participation should evolve into a collaborative effort with others. Because, while government and industry bicker about who takes the lead in this effort, a Middle-Eastern terrorist could be booting up his laptop to infiltrate our defenses with a few clicks of the mouse.

In a *60 Minutes* feature on cyber-warfare last April, National Coordinator of Security, Infrastructure Protection, and Counter-terrorism Dick Clarke, whose letter to *CPM* readers appears in ["A Challenge from Washington"](#), stated, "The owners and operators of electric power grids and pipelines and banks and railroads—they're the ones who have to defend our infrastructure. The government doesn't own it. The government doesn't operate it. The government can't defend it. This is the first time where we've had a potential foreign threat to the United States where the military can't save us."

It is indeed the responsibility of the private sector to ensure that our electronic borders are protected. Working together with competing businesses and with the government may not feel like the natural or comfortable thing to do, and it will certainly take some time, effort, and even caution, but as ["FS/ISAC: A Group Effort"](#) demonstrates, it is doable and is being done to the benefit of those businesses involved.

America is facing new threats. Let this supplement serve as a call to action for your company to join in the effort to protect our national and corporate interests against them.

A handwritten signature in black ink, appearing to read "Andy Hagg". The signature is written in a cursive style with a large, stylized initial "A".

Andy Hagg

Editor