



Information Age Insecurity



This is a simple text annotation



The **Information Age** is irrevocably altering the means by which the Government must approach the challenge of protecting its information. Protection no longer equates to placing documents in filing cabinets with strong combination locks. Instead, information vital to the security and continued prosperity of the United States resides in a series of increasingly interconnected classified and unclassified systems. The Commission believes that the findings and recommendations noted below provide policymakers the means to begin protecting information properly now and into the next century.

This is an era of extraordinary change not only in information technology, but also in the very way in which individuals communicate with one another. The Commission's goal is not to predict the future that these technological changes will help mold. Rather, it is to better understand the nature of the new threats so that the Government, with the full support of the private sector, can mitigate or prevent them.

At present, there exists what appears to be a growing gap between technological change and the human capacity to adapt to that change. The risk is that the Government will make bad decisions not because it has too little information, but rather because it has too much information about the wrong things. In such a rapid-paced and changing environment, it is only natural to fall back on old biases, protocols, and shortcuts. Convictions, as Nietzsche once noted, can be "more dangerous enemies of truth than lies."

Federal Government Information Security and the National Information Infrastructure

The information revolution, characterized by the growing convergence of computer and communications technologies, requires a fundamental rethinking of traditional approaches to safeguarding national security information. Those responsible for the protection of national security face new, increasingly difficult challenges presented by the proliferation of computer networks linked by telephone lines, cable, direct broadcast service, and wireless communications, and by the replacement of the traditional computer mainframe by personal computers. In this new electronic world—the National Information Infrastructure (NII)—best symbolized by the steadily growing global Internet, it is not clear what responsibility the Federal Government has to protect the infrastructure that stores, carries, and transmits nearly all of the Government's unclassified and classified information.

The NII within the ~~United States~~ is only one portion of the Global Information Infrastructure (GII) that connects public and private computer networks around the world. For the Federal Government to assume a leadership position in protecting the NII,