



The Use of Pearl Echo to Assist in Compliance with The Federal Information Security Management Act

The Federal Information Security Management Act (FISMA) was enacted in December 2002 as part of the E-Government Act of 2002. The purpose of FISMA is to provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets. The law applies to Federal information systems as well as information systems provided or managed by another agency, a contractor or other source.

Title III of FISMA, Information Security, addresses protecting information and information systems from unauthorized access, use, *disclosure*, disruption, modification, or destruction in order to provide *confidentiality*. Confidentiality is defined to mean preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.

Disclosure

Disclosure of data can take on many forms including the electronic transmission of nonpublic personal or proprietary information through e-mail, chat rooms, instant messaging and public news group postings. Pearl Echo's keyword blocking capability can be employed to prevent the dissemination of personal or proprietary information through any of these protocols. Pearl Echo can also be used to monitor the communications of individuals in order to identify the intent to access and distribute nonpublic personal or proprietary information before it occurs.

Confidentiality

Pearl Echo's control profiles provide the ability to define rules determining which users have access to specific areas of the organization's intranet. By creating access profiles within Pearl Echo, organizations will not only be able to control which individuals have access to personal or proprietary data through the organization's intranet, but will be able to audit who, internally, is attempting to fallaciously access personal or proprietary data.

