Legislative Summary: EEA

Making sure it's secure.™

Economic Espionage Act (EEA)
Enacted: October 11, 1996 (USA)

1 What the law covers:

- Owner protection against an individual or organization that knowingly, or conspires to, steal, copy, receive, buy, possess, alter or destroy their trade secret(s).

2 What are trade secrets:

- All forms and types of financial, business, scientific, technical, economic or engineering information where the owner has taken reasonable measures to keep secret
- The information derives economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means, by the public
- The information can be physical, electronic, graphical, photographical or written

Examples of trade secrets:

- Patterns
- Plans
- Compilations
- Program devices
- Formulas
- Designs
- Prototypes
- Methods
- Techniques
- Processes
- Procedures
- Programs
- Codes

3 Who is covered by the Act:

All individuals and organizations in the United States

4 How it relates to information management:

The purpose of the EEA is to protect trade secrets from being maliciously compromised. However to be defined as a trade secret, Section 1839 of the Act stipulates that the owner must be able to show they took "reasonable measures" to protect the information.

Secure document retention and disposal guidelines allow organizations to:

1. Reduce their risk of a security breach

2. In the event of a breach, be in a better position to show the FBI the reasonable measures taken to protect their trade secrets

5 How to comply:

No compliance regulations exist under the Act, but organizations can take recommended proactive measures to protect their trade secrets.

For more information:

Economic Espionage Act
www.economicespionage.com/EEA.html

6 How to implement protective measures:

Recommended secure document retention and disposal guidelines include:

Establish

- A detailed document retention and disposal policy
- Categories of trade secret information, the forms and level of protection required
- Protocols and restrictions on the access and sharing of trade secret information
- Policies for secure storage and proper disposal
- Procedures for staff training

Monitor

- End-to-end compliance – on a continual basis

Remember, trade secrets can be stored in many forms:

- As hard copy documents and files
- On CDs, cassettes, hard drives

7 Offences/penalties for infringement:

Who can be charged?

- Any individual or organization in the United States

What are the maximum penalties?

Economic Espionage
(Section 1831; benefits a foreign entity)

- Individual – fine: $5 million (or twice the loss/gain) and/or imprisonment: 15 years
- Organization – fine: $10 million, or three times the value of the stolen trade secrets, or twice the loss/gain (whichever is greater)

Theft of Trade Secrets
(Section 1832; injures owner)

- Individual – fine: $250,000 (or twice the loss/gain) and/or imprisonment: 10 years
- Organization – fine: $5 million (or twice the loss/gain)

In addition, offenders must pay restitution and face confiscation of any property derived from the offense. They may also be prosecuted under other federal statutes.

8 How Shred-it can help:

Secure Document and Hard Drive Destruction

- Secure end-to-end chain of custody
- Certificate of Destruction after every service
- Tailored solutions to your organization's needs

Advice and Expertise

- Trained experts in information security
- Provide a Risk Assessment Survey at your organization
- Helpful resources available at shredit.com/resource-center