



Federal Government Policies

Overview

The Sentrion Federal Government Policies Application plays a crucial role in national security. These policies are designed to control the flow of emailed information in violation of International Traffic in Arms Regulations (ITAR), as required by the U.S. Arms Export Control Act. The application also monitors the email stream to prevent controlled information from illegally flowing to countries listed by the U.S. State Department as State Sponsors of Terrorism.

Audience

Any researcher, manufacturer, exporter, or broker that deals with defense articles, services, or related technical data as defined by the U.S. Munitions List, as well as government agencies with missions that relate to national security—for example, the Department of Energy and NASA.

Key Features and Functionality Overview

The purpose of ITAR is to control the export of any technology or related information that could have a military application until it has been vetted by the Department of Commerce. ITAR first went into effect in 1976, during the Cold War. Since that time, however, enforcement has become exponentially more difficult—and more essential—due to two trends.

First, the threat landscape has become decentralized as traditional Cold War rivalries have given way to independent, globally distributed and highly mobile terrorist cells. Second, and even more challenging, the ascent of global computing and communications technologies has virtually eliminated international borders. That means information can fall into the wrong hands, anywhere in the world, at the click of a mouse. For a company with international clients and even internal employees stationed both in the U.S. and overseas, consider how easy it would be to leak vital national security information simply by inadvertently including the wrong person on an email distribution list.

Sentrion Federal Government Policies are designed to prevent ITAR-controlled information from reaching unauthorized people within or beyond your organization via email, even including non-citizens within the U.S. The application works directly within the mail stream, so you can count on proactive policy enforcement without the need to adapt an add-on DLP solution using proxies or complicated sandwich configurations. When a violation is detected in the email body or any attachment, the application takes action based on your custom policies for example:

- Block the message and notify the sender of the violation
- Quarantine the message and create an entry in the Incident Remediation and Reporting Application for further review
- Encrypt and send the message using the using Voltage or S/MIME Encryption

Sentrion Federal Government Policies can also be used to prevent classified information from flowing from networks with higher classifications to lower classifications. Our Professional Services team customizes the solution to your business and security needs, no matter what types of sensitive information you deal with, and no matter where your offices and clients are located.

The U.S. Government has stepped up ITAR audit and enforcement in recent years, levying severe financial penalties in several high-profile cases. Why take a chance? Put forward your best defense: Sentrion Federal Government Policies.