SECTIGO

Meeting Federal Requirements for Secure Email

Compliance to Defense Federal Acquisition Regulation - Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

For many years the United States government has been under constant cyberattack to steal intellectual property such as the designs of America's best military assets. As government agencies have improved their cyber defense, attackers have increasingly shifted focus to U.S. defense contractors to gain access to information of strategic national importance. These attacks include stealing the weak credentials of employees to access contractor systems remotely and stealing the intellectual property stored in email, either in transit or stored on the mail server.

To remedy this situation, the government added section 252.204-7012 to the Defense Federal Acquisition Regulation. This regulation requires compliance with NIST SP800-171 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.

Sectigo is the leading provider of strong digital identities using public key technology. These identities are valuable for a wide range of applications in the enterprise, from mobile device authentication in wireless networks to encrypting and digitally signing emails using the popular S/MIME standard.

For cyber defense to be effective, it must be invisible, easy for the administrator to deploy and easy for the employee to use. Unfortunately, previous S/MIME solutions were too difficult to use, with the result being that employees failed to encrypt their email. This poor security solution opened the entire system to attacks.

To solve this problem Sectigo developed the industry's first zero touch, X.509 certificate management system. This system provisions digital identities automatically to any application using traditional windows devices or mobile devices.

A single administrator console allows for the provisioning of both publicly trusted S/MIME certificates and private certificates dedicated to the exclusive use of the enterprise. The console allows for control over employee, server, and device enrollment. It effortlessly provides discovery, reporting, automated renewal without employee involvement, and revocation when the employee leaves. The console enables crypto-agility using renewal on demand, including the ability to increase the cryptographic strength of the identity.

The console automatically adopts all previous issued certificates to dramatically improve deployment, with the most popular being the certificates issued by the corporation's Active Directory Certificate Service. These certificates can then be automatically replaced by publicly trusted S/MIME certificates. Public S/MIME allows for any S/MIME capable mail application to validate the sender's identity and also that the email and its attachments have not been altered in transit. This same solution enables compliance to International Traffic in Arms Regulation.

To truly enable nearly 100% of emails to be encrypted, the solution adds these important features ignored by previous S/MIME solutions:

- **Sending the entire encryption key history to all mails apps so even older emails can be decrypted**
- **Encryption key archiving so the employee can recover accidentally destroyed keys**
- **Interoperation with the secure email gateways so that the enterprise may still use mail scanners to perform their functions on encrypted and signed emails**

To learn more about how zero-touch S/MIME certificates can help you protect your business and meet federal compliance requirements, contact Sectigo today.

