thalescpl.com

THALES

10 Things to Know
Are you DFARS Ready?

1). What is DFARS?

DFARS (Defense Federal Acquisition Regulation Supplement) is an addition to the Federal Acquisition Requirement (FAR) and provides specific acquisition regulations for the Department of Defense (DoD).

2). Who does it affect?

DFARS applies to DoD government acquisition officials, as well as any contractors doing business with the DoD. DFARS rules focus on systems with CDI (Covered Defense Information) not just the specific information. "Covered Contractor Information Systems" means information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information. Any contractor or subcontractor who comes in contact with a CDI.

3). What are the goals of DFARS?

To address the need to increase the cyber security requirements on information held by contractors. DFARS requires contractors to comply with National Institute of Standards (NIST) Special Publication 800.171 to protect Controlled Unclassified Information (CUI). NIST 800-171 describes a series of procedures for "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations."

4). Deadline to comply:

Dec. 31, 2017. The Pentagon twice pushed back the original date to give more time to contractors who were struggling to meet the government requirements so quickly.

5). What happens if you don't comply or make a false claim?

Non-compliance could result in criminal, civil, administrative, and contractual actions (governed by specific contract) in law and equity for penalties, damages, and other appropriate remedies.

6).What about the DFARS 7012?

DFARS clause 252.204-7012 was added and structured to ensure unclassified DoD information residing on a contractor's internal information system is safeguarded from cyber incidents, and that any consequences associated with the loss of this information are assessed and minimized via the cyber incident reporting and damage assessment processes. With this clause come additional security requirements, most notably the addition of multi-factor authentication as a minimum security standard.

7). Controlling physical access

DFARS extends to controlling access to physical locations and documents 3.10 PHYSICAL PROTECTION Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

8). Addressing identification and authentication requirements

Section 3.5 of NIST 800-171 addresses Identification and Authentication. Among other things this section mandates:

Multifactor authentication

3.5.3 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.

Multifactor authentication ensures a user is who they claim to be. Multifactor authentication can be achieved using a combination of the following factors something you have (such as a token or smart card), with something you know (PIN or password) and/or something you have (biometric). The more factors used to determine a person's identity, the greater the trust of authenticity.

Replay-resistant authentication

Two-factor authentication using smart cards or one-time password tokens prevents this type of attack because you need to present a secondary form of authentication.

9). How Thales's Access Management and Authentication Portfolio can help

Authentication

Offering the broadest range of authentication methods and form factors, SafeNet authentication solutions allows customers to address numerous use cases, assurance levels, and threat vectors with unified, centrally managed policies— managed from one authentication back end delivered in the cloud or on-premises. Supported authentication methods include context-based authentication combined with step-up capabilities, OOB, one-time password (OTP), and X.509 certificate-based solutions. All authentication methods are available in numerous form factors, including smart card, USB token, software, mobile app, and hardware tokens.

Physical Access

Thales offers an assortment of smart cards with dual physical and logic access (multifactor authentication), including contact cards with a wide choice of card body options and contactless technologies and dual interface cards compatible with NFC.

For DFARS, Thales recommends a FIPS certified smart card with a hybrid option for physical and logical access, offering a cost solution to meet all DFARS requirements.

Privileged Access

In addition to basic identification, Thales's Authentication solutions offer a complete set of provisioning rules and policy engines that cover privileged users and what level of security is needed for these roles. The more critical and private the data, the more security needed to access.

10). Why Thales?

Thales offers the only complete portfolio of Authentication and Access Management solutions, including cloud access Management, PKI, certificatebased authentication, one-time password authentication, identity federation, complete lifecycle management and auditing tools.

Thales also has data protection and encryption tools that work together with our Authentication and access management solutions to provide persistent protection and management of sensitive data, which can be mapped to the DFARS framework.

© Thales - Jul2019 • EH v1

> thalescpl.com <

Americas – Thales eSecurity Inc. 2860 Junction Ave, San Jose, CA 95134 USA • Tel:+1 888 744 4976 or +1 954 888 6200 • Fax:+1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific – Thales Transport & Security (HK) Lt, Unit 4101-3, 41/F, Sunlight Tower, 248 Queen's Road East, Wanchai, Hong Kong • Tel:+852 2815 8633 • Fax:+852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa – Meadow View House, Long Crendon, Aylesbury, Buckinghamshire HP18 9EQ • Tel:+44 (0)1844 201800 • Fax:+44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com