SAASPASS

DFARS NIST 800-171 Compliance

What is DFARS NIST 800-171?

In 2010, President Obama issued Executive Order 13556 to begin harmonizing the patchwork of different policies pertaining to controlled unclassified information (CUI) across federal departments and agencies. On the basis of this program, the Department of Defense (DoD), General Services Administration (GSA), and NASA collaborated to publish a DFARS update mandating that any non-federal entity handling CUI must comply with the security guidelines in Special Publication 800-171 issued by the National Institute of Standards & Technology (NIST).

Deadline for compliance : December 31, 2017

What are the DFARS NIST 800-171 requirements?

The major update to earlier DFARS versions is the multifactor authentication (MFA) requirement, but there are a total of 14 families of specific security requirements included in NIST 800-171: Access Control, Awareness and Training, Audit and Accountability, Configuration Management, Identification and Authentication, Incident Response, Maintenance, Media Protection, Physical Protection, Personnel Security, Risk Assessment, Security Assessment, System and Communications Protection, and System and Information Integrity.

Who's impacted?

Government contractors, universities and research organizations receiving federal grants, law enforcement agencies, state and local governments, and any other non-federal entities who process, store, or transmit sensitive but unclassified data (CUI) from DoD, GSA, NASA, or other federal or state agencies. Entities who don't comply with these security requirements by the deadline risk termination of contract.

IMPORTANT: DFARS NIST 800-171 Offline MFA requirements

Before selecting a service provider to help comply with DFARS NIST 800-171, be sure to ask about a vendor's offline MFA requirements, as most do not have this capability. Not only is offline MFA important for protecting data against physical threats, but the ability to secure a privileged user's computer with MFA even while offline is explicitly listed in NIST 800-171 requirement 3.5.3:

> *3.5.3 Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.*
>
> *'Local access' is any access to a system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network.*

SAASPASS, 44 Tehama Street, San Francisco, CA 94105 • **888-512-SAAS**

SAASPASS

What is SAASPASS?

SAASPASS is a San Francisco-based security and identity solution provider. Instead of stitching together two or more point solutions for multi-factor authentication, single sign-on, endpoint access, password management, and even physical control access, SAASPASS is the only comprehensive full-stack identity and access management solution on the market. No other single product meets all of your identity needs, meets them with greater convenience and ease-of-use, at reduced total cost, and without leaving holes in your digital security, such as when devices are offline. SAASPASS even locks down Macs.

The SAASPASS Advantage

- Meets all DFARS NIST 800-171 MFA requirements (both online and offline)
- Secures Macs and PCs
- Single sign-on access to hundreds of enterprise applications (Salesforce, Office 365, etc)
- Simple to implement
- Easy to use
- Scalable (pay for what you use)
- Reduces security complexity

Pricing

SAASPASS uses a subscription-based pricing model, with a two month free trial. Please visit www.saaspass.com/pricing for the latest pricing information.

Don't Wait Until December 31st to Get Started

Contact sales@saaspass.com for a demo or for help with implementation.

...or simply start right away on your own by following these steps:

1. Download SAASPASS app onto mobile device
2. Register company/organization through the mobile app or from computer
3. Go to the admin portal and begin setting up groups and users
4. Verify users with their corporate email or with a CSV upload
5. Roll out SAASPASS Computer Connector to the machines you need secured, once users have paired their accounts to SAASPASS IDs

For any technical questions, please contact support@saaspass.com

SAASPASS, 44 Tehama Street, San Francisco, CA 94105 • **888-512-SAAS**