CASE STUDY

Smart Access
Cyber Access Control

Government Contractor Required MFA for DFARS Compliance

As a manufacturer and sub-contractor to DoD projects, we are required to meet the DFARS compliance to NIST SP 800-171, where we must implement Multi-Factor Authentication as part of our overall cybersecurity strategy. If sensitive data access is not secured with at least two-factor authentication, we run the risk of being dropped as a government supplier. Power LogOn fulfils their 2FA requirement by authenticating that an individual is allowed access to sensitive data, and Power LogOn keeps an audit record of all computer and data access should a problem occur.

Security Challenges

- **NIST 800-171, 800-63, and 800-53 Compliance**
  DFARS states that government contractors and suppliers must address these three specifications to meet the MFA cyber security requirements.

- **No smartphones allowed**
  Our employees are not allowed to have any smartphones or mobile devices on the manufacturing floor. This makes it impossible for us to implement any SMS, email, or smartphone authenticator app for MFA..

- **One credential for both physical and cyber access control**
  For employee convenience, we want one ID badge that combines both building access, and computers, data files, and CNC machines log in. If the card can also auto-log off the user when removed, that too would be a great security feature.

The Solution

Already in use: 13.56MHz building access cards

Purchased: Embed a Java smartcard module, contact smartcard readers, Power LogOn software and licenses, and a support contract.

Here are some key Power LogOn highlights that solved their challenges:

1. **IT Centrally Managed Passwords**
   All the employees logons passwords are now centrally managed by IT, without employee involvement. IT also creates different user groups depending on an

employee's responsibility. Now authentication follows DFARS policies that employees cannot circumvent.

2. **Government Compliance**

   Power LogOn is compliant with the DFARS MFA security specifications like: NIST 800-53, 800-63, 800-171, and FIPS 140-2.

3. **A True multi-factor authentication solution**

   True MFA is when employee presents two or more dissimilar factors. For Example, a card (the Possession factor), and a PIN (the Knowledge factor). Power LogOn uses this information to auto fill in a secure username and password to access a Window's computer and server without the employee knowing or typing any passwords.

4. **No smartphone allowed**

   Because the customer doesn't allow smartphones or mobile devices in the manufacturing area, Power LogOn leverages their existing access control ID badges to access computers, CNC machines, and data files.

5. **Usage Audit Trail**

   Power LogOn records employee logon activities. At any given time, IT can view exactly which employees accessed which workstations and data.

Customer Feedback

We talked to many of the leading access control companies, and none offered an affordable and easy solution. Then we discovered Power LogOn. We bought their pilot kit and was hook by the first day. We now are compliant with the MFA DFARS requirement.

Power LogOn Administrator Integration Kits

Test Power LogOn for 90-days at no risk. We offer different configuration options

Contact Smartcard version

Contactless Smartcard version