DFARS 252.204-7012 Requirements for Defense Contractors Must Be Satisfied by DECEMBER 31, 2017

As with most government documents, one often leads to another. And that's the case with DFARS 252.204-7012 . "DFARS" (the Defense Federal Acquisition Regulation Supplement Part 252: Solicitation Provisions and Contract Clauses) states:

> "Contractors shall implement NIST SP 800-171 as soon as practical, but no later than December 31, 2017."

That leads us to the next document: NIST Special Publication 800-171: Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations. This document was originally written as *suggested* ways to protect data. The DFARS document is now *requiring* the NIST suggestions.

THE PROBLEM

Defense contractors, including the small companies that supply the big ones, must implement DFARS requirements or they will be dropped as suppliers. Not having these measures in place could put a company out of business. That's why DFARS is such an urgent issue.

One area of concern that defense contractors face happens on the assembly floor. Manufacturing facilities often have centrally located computers accessed by multiple users. Currently, workers are typing a user name and password to log in. If their passwords are compromised, or if an employee shares their passwords, there is no way for that current system to verify who actually logged in, which does *not* meet DFARS.

Part of the DFARS includes having an authentication process, plus a tracking ability.

AUTHENTICATION

The Power LogOn system utilizes a smartcard as one factor of the Multi-Factor Authentication process (something you Have). The card is protected by a PIN (a second factor - something you Know.) Because the user doesn't even know their passwords, there is nothing they can share or tell to allow another person to be able to log in. The card allows you to know absolutely that it was Joe's card that logged in.

The PIN protected card adds a layer of assurance, creating Two Factor Authentication, which does meet DFARS. For a super secure site, another layer could be added using a biometric, (something you Are - which our software supports), creating Three Factor Authentication.

2 Factors = Card + PIN (most cost effective and fastest to implement) or
Card + Biometric

3 Factors = Card + PIN + Biometric

The more hurdles you put up, the harder it becomes for a hacker or thief.

TRACKING and REPORTS

Power LogOn records whose card comes into the system, what that person logged into, how long they were in, and when they logged out. This process leaves an audit trail, which is also required in the DFARS.

DIFFERENTIATION

What makes Power LogOn so much better than other solutions is that the defense contractor doesn't have to go through the complexity or expense of certificates and PKI. They can add the Power LogOn system directly onto their existing physical access badges, creating even more benefits. Because physical access badges are often used for more than just door access - think time and attendance, payment in cafeterias, forklift ignition, etc. - there are a lot of different cross references and cross checks. If Joe logs into the system, but Joe has not clocked in or come through the door, that becomes a system red flag.

COMPLIANCE

Here's a list of DFARS requirements that defense contractors are trying desperately to comply with by the end of THIS YEAR. *Power LogOn meets each section with a check mark*.*

3.1 ACCESS CONTROL			
Basic Security Requirements:			
		Power LogOn Feature	
3.1.1	Limit system access to authorized users, processes acting on behalf of authorized users, or devices (including other systems).	1. Users don't know passwords. 2. Logon user names and passwords are auto-filled 3. Uses MFA to log in. 4. IT configures which users have access to which accounts, networks, clouds, etc. 5. Coordination with LDAP systems like Active Directory	✓
3.1.2	Limit system access to the types of transactions and functions that authorized users are permitted to execute.	1. IT configures which users have access to which accounts, networks, clouds, etc. by means of IT managed User Groups and the management of those groups. 2. Requires MFA to log in. 3. Coordination with LDAP systems like Active Directory	✓
Derived Security Requirements:			
3.1.3	Control the flow of CUI in accordance with approved authorizations.	1. Users don't know passwords. 2. Utilizes MFA to log in. 3. IT configures access.	✓
3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	1. Employees are required to use an issued smartcard on their ID badge. 2. Users don't know or manage any account passwords. Handled by IT. 3. IT determines the length, complexity, uniqueness and change frequency without user involvement. 4. Different User Groups can be setup where each have different access rights and privileges. 5. Coordination with LDAP systems like Active Directory	✓
3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts.	1. Multiple User Groups can be setup where each have different access rights and privileges. 2. IT determines the length, complexity, uniqueness and change frequency without user involvement.	✓
3.1.6	Use non-privileged accounts or roles when accessing non-security functions.	1. Using MFA to identify individual at computer bootup to identify user. 2. User privileges based on IT controlled User Group. 3. Coordination with LDAP systems like Active Directory	✓
3.1.7	Prevent non-privileged users from executing privileged functions and audit the execution of such functions.	1. Using MFA to identify individual at computer bootup to identify user. 2. Users don't know passwords. 3. User privileges based on IT controlled User Group. 4. Coordination with LDAP systems like Active Directory 5. Audit reports that show person, day, time of logon and logoff	✓
3.1.8	Limit unsuccessful logon attempts.	1. Logon requires a card and PIN. Four wrong PIN entries will block the card and notify engineering. 2. Users don't know any account passwords so they can't enter them or share them.	✓

3.1.9	Provide privacy and security notices consistent with applicable CUI rules.	1. Reports 2. Cardholder Report: If they are users or administrators, active or inactive, hot listed or not hot listed. 3. Transaction report: Date, time, transaction type, User ID, cardholder ID, card ID, and workstation ID. 4. Text file that can be combined with other reporting software.	✓
3.1.10	Use session lock with pattern-hiding displays to prevent access and viewing of data after period of inactivity.	1. Display can be set to lock. 2. Card re-authentication time can be set. 3. Card removal can be set to lock session instantly.	✓
3.1.11	Terminate (automatically) a user session after a defined condition.	1. When the card is removed, the session is terminated and the user is logged off, computer locked, computer shuts down, or custom script.	✓
3.1.12	Monitor and control remote access sessions.	1. Reports monitor who and when a user logs on and off 2. Works with terminal services and remote desktop to control access. 3. Card can be used to logon from any remote computer with the Power LogOn software and reader. 4. Password transmission encrypted between client and server	✓
3.1.13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.	1. Employees don't know, type, or manage any passwords 2. Every account has its own unique password 3. Passwords are encrypted using SHA-256 and AES-256 4. SSL between client and server to block man-in-the-middle attacks	✓
3.1.14	Route remote access via managed access control points.	1. Computer becomes the control point. We do this by: a. MFA (Card + PIN, Card + Biometrics, or Card + PIN + Biometrics). b. Ties into Remote Desktop and Terminal Services. c. Password encryption between client and server. d. Ties into Active Directory or other LPAD systems.	✓
3.1.15	Authorize remote execution of privileged commands and remote access to security-relevant information.	1. Utilizes MFA 2. User needs MFA to log onto computer during bootup so a trusted node is seen on the network. 3. User doesn't know or manage any logon passwords. 4. Password encryption between client and server	✓
3.3 AUDIT AND ACCOUNTABILITY			
Basic Security Requirements:			
3.3.1	Create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity.	1. Cardholder Report: If they are users or administrators, active or inactive, hot listed or not hot listed. 2. Transaction report: Date, time, transaction type, User ID, cardholder ID, card ID, and workstation ID. 3. Text file that can be combined with other reporting software. 4. Lost, forgotten, or stolen cards are hot listed and blocked from access to network.	✓

3.3.2	Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	1. Cardholder Report: If they are users or administrators, active or inactive, hot listed or not hot listed. 2. Transaction report: Date, time, transaction type, User ID, cardholder ID, card ID, and workstation ID. 3. Text file that can be combined with other reporting software.	✓
Derived Security Requirements:			
3.3.3	Review and update audited events.	1. Records are always active and available 2. Records can be exported to other third-party record programs.	✓
3.3.4	Alert in the event of an audit process failure.	1. Reports and transaction records are always available in real time, so always available for an audit. 2. Report data can be exported to third party reporting software.	✓
3.3.5	Correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.	1. Records are always active and available 2. Records can be exported to other third-party record programs.	✓
3.3.6	Provide audit reduction and report generation to support on-demand analysis and reporting.	1. Records are always active and available 2. Records can be exported to other third-party record programs.	✓
3.3.7	Provide an information system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.	1. Uses Microsoft time and date feature	✓
3.3.8	Protect audit information and audit tools from unauthorized access, modification, and deletion.	1. Admin needs to log into the management software to access reports. 2. Logon can be done using the same MFA card that access any other account. 3. Passwords are typically set to 20 alpha-numeric-special characters long	✓
3.3.9	Limit management of audit functionality to a subset of privileged users.	1. IT creates user group for only those authorized to access audit functionalities.	✓
3.4 CONFIGURATION MANAGEMENT			
Basic Security Requirements:			
3.4.1	Establish and maintain baseline configurations and inventories of organizational systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	1. We use industry standard, non-proprietary cards and readers 2. Works with over fifty different card technologies. 3. Cards can be anything from magnetic stripe, contact smartcards, or contactless cards (Prox, iClass, DESFire, Mifare) 4. Work with numerous reader technologies that are PC/SC compliant	✓
3.4.2	Establish and enforce security configuration settings for information technology products employed in organizational systems.	1. Secure card issuance and management software 2. IT enforces security configurations that users are not allowed to circumvent. 3. IT determines length, complexity and change frequency without user involvement 4. Create different User Groups each with their own security configurations	✓
Derived Security Requirements:			

3.4.3	Track, review, approve/disapprove, and audit changes to organizational systems.	1. Report tracks issuance, hot listing and revoking cards from system. 2. Reports the actions taken by administrators 3. Text file that can be combined with other reporting software.	✓
3.4.6	Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	1. IT can configure and manage what features and capabilities the user can perform.	✓
3.4.8	Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny-all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.	1. Card management allows IT to hot-list cards so they will no-long be allowed access. 2. Because user does not know their passwords, no back door. 3. Because IT can change any password without user involvement, again no back door	✓
3.5 IDENTIFICATION AND AUTHENTICATION			
Basic Security Requirements:			
3.5.1	Identify system users, processes acting on behalf of users, or devices.	1. Multi-factor Authentication options (card + pin, card + biometrics, or card+pin+biometrics) 2. Mutual Challenge and Response between card and server 3. MFA utilized at computer bootup, before the firewall. Creates a trusted node into server. 4. After MFA authentication computer and account user name and passwords are auto-filled into logon screens 5. User identification is established each and every time the user accesses a computer, application, server, cloud, and web site.	✓
3.5.2	Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational systems.	1. User authenticates to the card 2. Card authenticates to Windows logon at bootup 3. After computer authentication, the user authenticates into applications, servers, clouds and websites by double-clicking.	✓
Derived Security Requirements:			
3.5.3	Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	1. User to Card MFA: Card, PIN and biometrics 2. Card to Computer MFA: Card, Decryption keys, CUID 3. Logon to computer, applications, websites, servers, cloud, and networks	✓
3.5.4	Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	1. Passwords are not cached	✓
3.5.5	Prevent reuse of identifiers for a defined period.	1. Centralized card management 2. Hot listed credential	✓
3.5.6	Disable identifiers after a defined period of inactivity.	1. Hot list credential	✓
3.5.7	Enforce a minimum password complexity and change of characters when new passwords are created.	1. IT centralized password configuration 2. Configure password min/max length, character types, change frequency. 3. Lockable so user cannot change settings	✓
3.5.8	Prohibit password reuse for a specified number of generations.	1. Centralized card management 2. Password reuse is set within the Power LogOn card management software	✓
3.5.9	Allow temporary password use for system logons with an immediate change to a permanent password.	1. IT sets and issues the temporary password with Power LogOn	✓

3.5.10	Store and transmit only cryptographically-protected passwords.	1. Uses AES-256, SHA-256, and SSL encryption for storage and transmission. 2. Password are not cached 3. FIPS 140-2 certified encryption algorithms.	✓
3.5.11	Obscure feedback of authentication information.	1. Password are obscured during auto-entry 2. Password obscured in account viewing 3. Passwords can be set so user can not view or change passwords.	✓
3.8 MEDIA PROTECTION			
Basic Security Requirements:			
3.8.1	Protect (i.e., physically control and securely store) system media containing CUI, both paper and digital.	1.Digital media is protected by means of authentication, authorization, and verification of user. 2. When credential is removed from reader, the computer with shut down, log user off, lock computer, or run a custom script.	✓
3.8.2	Limit access to CUI on system media to authorized users.	1.IT creates user groups to determine who has access to digital media. 2. Digital media is protected by means of authentication, authorization, and verification of user. 3. When credential is removed from reader, the computer with shut down, log user off, lock computer, or run a custom script.	✓
3.8.9	Protect the confidentiality of backup CUI at storage location	1. Power LogOn protects digital media backup by authenticating authorized users only. 2. IT controls and manages user groups who have access to confidential CUI at storage location.	✓
3.9 PERSONNEL SECURITY			
Basic Security Requirements:			
3.9.1	Screen individuals prior to authorizing access to organizational systems containing CUI.	1. Power LogOn tied to the employee badge, which required screening before issuance to user.	✓
3.9.2	Ensure that CUI and organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.	1. Card can be hot listed immediately upon personnel actions, such as termination. 2. IT can transfer an end user from one User Group to another instantly	✓
3.10 PHYSICAL PROTECTION			
Basic Security Requirements:			
3.10.1	Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.	1. Power Logon can be added to existing physical access credential for convenience to user and management by IT	✓