Achieving Cybersecurity Maturity Model Compliance

WHITE PAPER

1. Introduction

The Cybersecurity Maturity Model Certification (CMMC) is a certification and compliance process developed by the Department of Defense (DoD).

Released in January 2020, CMMC brings together a collection of compliance processes namely NIST SP 800-171, NIST SP 800- 53, ISO 27001, ISO 27032, and AIA NAS9933 to certify that contractors have the controls in place to protect sensitive data.

CMMC requires DoD contractors to have their systems audited by a 3rd party. The contractor remains responsible for the implementation, monitoring, and certification of the appropriate cybersecurity controls.

2. The 5 levels of CMMC

CMMC has 5 certification levels that reflect the maturity and reliability of a company's cybersecurity to protect sensitive government data on the organization's I.T. systems.

The 5 levels are as follows:

Level 1: Basic Cyber Hygiene

A company must perform "basic cyber hygiene" practices, such as using antivirus software and password complexity requirements required to protect the Federal Contract Information (information that is not intended for public release or certain transactional information).

Level 2: Intermediate Cyber Hygiene

A company must document certain "intermediate cyber hygiene" practices to begin to protect any Controlled Unclassified Information (CUI) through the implementation of some of the US Department of Commerce National Institute of Standards and Technology's (NIST's) Special Publication 800-171 Revision 2 (NIST 800-171 r2) security requirements.

CUI is "any information that law, regulation, or government-wide policy requires to have safeguarding or disseminating controls," but does not include certain classified information.

Level 3: Good Cyber Hygiene

A company must have an institutionalized management plan to implement "good cyber hygiene" practices to safeguard CUI, including all the NIST 800-171 r2 security requirements as well as the additional standards.

Level 4: Enhanced Cyber Hygiene

A company must have implemented procedures for defining and measuring the efficacy of implemented controls as well as establishing enhanced practices to detect and respond to changing tactics, techniques and procedures of advanced persistent threats (APTs).

An APT is defined as an adversary that possesses sophisticated levels of expertise and significant resources that allow it to create opportunities to achieve its objectives by using multiple attack vectors.

Level 5: Advanced Cyber Hygiene

A company must have standardized and optimized processes in place across the organization with enhanced controls that provide more sophisticated capabilities to detect and respond to Advanced Persistent Threats.

3. Compliance Using MyID PSM and MFA

MyID PSM and MFA provides multiple complementary solutions to assist companies in achieving Cybersecurity Maturity Model Compliance for all 5 levels of certification. CMMC is an amalgamation of numerous compliance publications that cater to all aspects of cybersecurity. Organizations are required to adhere to best-practice standards and additional supplementary compliance requirements that are outlined in these publications, with an ongoing commitment.

MyID PSM and MFA solutions have been designed to comply with best practices with a key focus on adhering to NIST compliance for password security and user authentication. Intercede has numerous tools and solutions to assist the organization to achieve CMMC and ensure on[1]going compliance with the framework. This is achieved with our Password Compliance and Multi-Factor Authentication solutions, both of which are prescribed requirements for secure and compliant environments.

4. Password Authentication Requirements

NIST Special Publication 800-53, a core component of CMMC, specifies authentication requirements and highlight the following password-based authentication requirements:

a) Maintain a list of commonly used, expected, or compromised passwords and update the list [Assignment: organization-defined frequency] and when organizational passwords are suspected to have been compromised directly or indirectly;

b) Verify, when users create or update passwords, that the passwords are not found on the organization-defined list of commonly used, expected, or compromised passwords;

c) Transmit only cryptographically protected passwords;

d) Store passwords using an approved hash algorithm and salt, preferably using a keyed hash;

e) Require immediate selection of a new password upon account recovery;

f) Allow user selection of long passwords and passphrases, including spaces and all printable characters;

g) Employ automated tools to assist the user in selecting strong password authenticators;

h) Enforce the following composition and complexity rules: [Assignment: organization-defined composition and complexity rules].

NIST Special Publication 800-63 (not specifically listed within CMMC directly, however is a standard referenced within SP 800-171 detailing best-practices for password security) goes into more detail and provides additional granularity regarding acceptable passwords. The high[1]level requirements specified within this SP state that passwords cannot be:

a) Passwords obtained from previous breach corpora;

b) Dictionary words;

c) Repetitive or sequential characters (e.g. ‘aaaaaa’, ‘1234abcd’);

d) Context-specific words, such as the name of the service, the username, and the derivatives thereof.

5. MyID PSM

The MyID Password Security Management (PSM) solution assists organizations to comply with the above requirements and includes comprehensive tamper-proof logging for audit and accountability with the use of the Intercede Password Breach Database.

Compromised passwords are detected through the Password Breach Database which is comprises of over 8 billion breached credentials, including over 3 billion unique clear text passwords. If a user selects a password that exists in the Password Breach Database, PSM will identify this password as being compromised and prevent usage of it accordingly. Without access to such a Password Breach Database, an organization will not be able to determine whether a password has been previously breached or not.

MyID PSM includes detailed and defined complexity checks allowing organizations to enforce stong and policy comliant passwords and deny the usage of passwords that fail the password checks. These checks include specifying minimum and maximum lengths, usage of month and day names, usernames or partial username, excessive sequential and repeated characters usage, and a whole host of additional rules ensuring sufficient password strength and NIST compliance.

In addition, the growing use of federated authorization services has to be recognized and accommodated where it is appropriate, with due consideration given to privacy and resilience.

6. Active Directory Password Auditing

Intercede's Active Directory Password Audit service is designed for an organization's to determine their current vulnerabilities and provide a detailed report outlining the risks and issues. The Audit tool is designed to be a non-intrusive process that checks for previously breached, shared passwords and highlights compliance issues against the NIST password policy standards. Running the AD Audit tool rcan help to ensure on-going compliance as per CMMC regulations.

7. MyID MFA

CMMC requires organizations to ensure that authentication is not solely limited to strong and secure passwords but also enforce additional secure authentication factors.

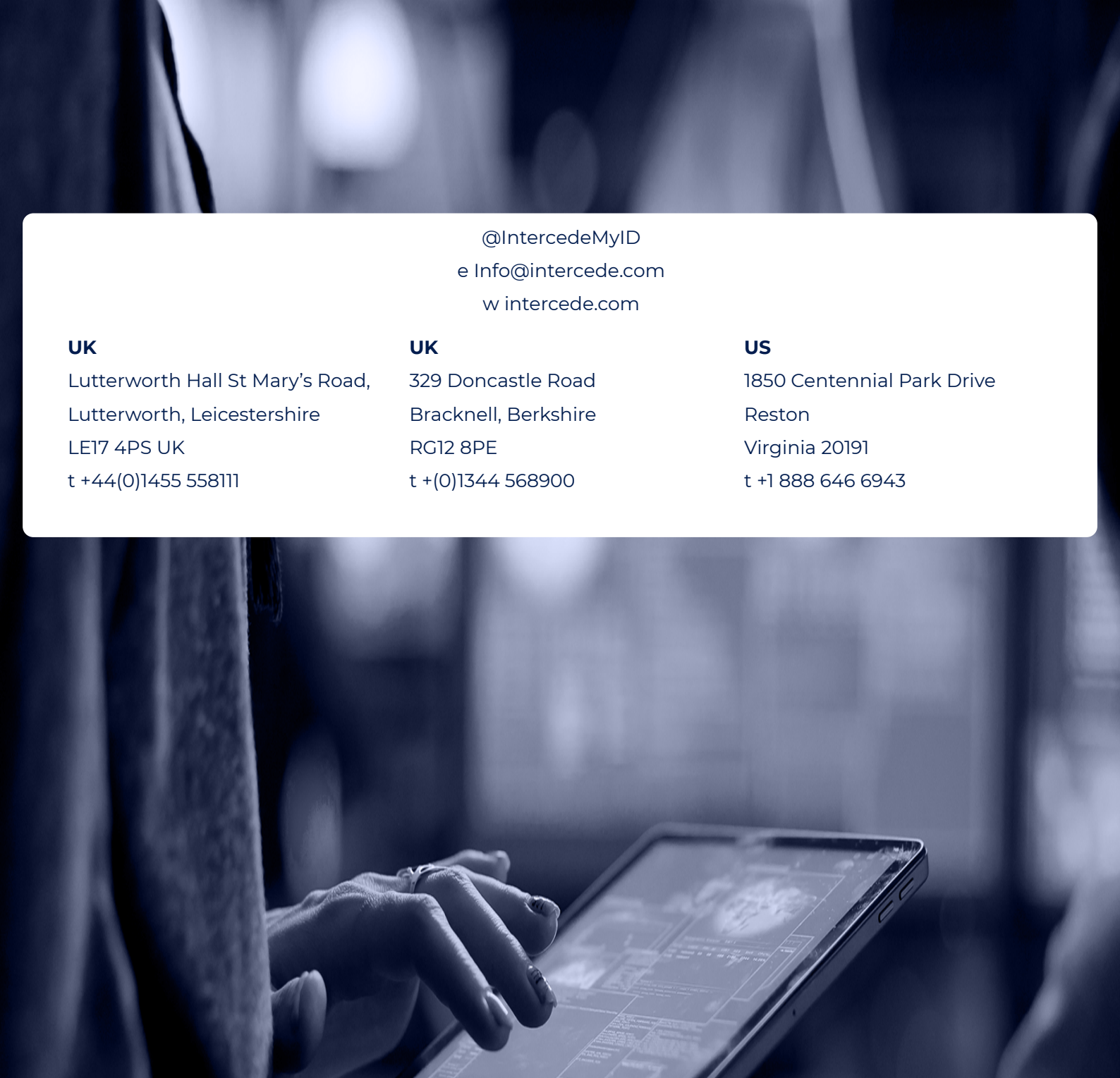
Multi-factor Authentication (MFA) solutions can be physical hardware authenticators, soft-tokens (mobile phone apps) that provide time-based or challenge-response authentication requests; and high-assurance phisihng-resistant authentication such as the U.S. Government Personal Identity Verification card or the DoD Common Access Card and FIDO passkeys.

CMMC breaks down MFA requirements for privileged accounts and non-privileged accounts. However, irrespective of the account and access type, both privileged and nonprivileged accounts must authenticate using multi-factor options appropriate for the level of risk. Organizations can add additional security measures, such as additional or more rigorous authentication mechanisms, for specific types of access.

8. Conclusions

MyID PSM and MFA provides a complete CMMC compliant cost-effective multi-factor authentication, password replacement, and single sign-on authentication solution for traditional desktops, over the phone or in the browser authentication.

Contact us today to arrange a demo.



@IntercedeMyID

e Info@intercede.com

w intercede.com

UK

Lutterworth Hall St Mary's Road,

Lutterworth, Leicestershire

LE17 4PS UK

t +44(0)1455 558111

UK

329 Doncastle Road

Bracknell, Berkshire

RG12 8PE

t +(0)1344 568900

US

1850 Centennial Park Drive

Reston

Virginia 20191

t +1 888 646 6943