THALES

www.thalesesecurity.com

COMPLYING WITH THE MINISTRY OF DEFENCE'S DEFCON 658

- Access control ensure only credentialed users can retrieve sensitive data
- Security intelligence logs identify irregular access patterns and breaches in progress
- Strong encryption and key management renders sensitive data useless to unauthorized users

‹Thales eSecurity›

HELPING SUPPLIERS COMPLY WITH THE UK MINISTRY OF DEFENCE'S DEFCON 658 REQUIREMENTS

Thales eSecurity's data security solutions provide the tools you need to demonstrate compliance with DEFCON 658 and that your business is viable to participate in valuable MoD contracts.

ABOUT DEFCON 658

The UK Ministry of Defence's DEFCON 658 is a procurement protocol on cybersecurity that requires all suppliers bidding on MoD contracts, which necessitate the transfer of MoD-identifiable information, to comply with the controls outlined in Defence Standard (DEFSTAN) 05-138. Notably, adherence to DEFCON 658 extends to the supply chains (sub-contractors) of the suppliers themselves.

This follows the establishment in 2013 of the Defence Cyber Protection Partnership (DCPP), a joint defence and supply chain initiative tasked with improving the protection of the defence supply chain from cyber threats. The DCPP defined both a cybersecurity model and a range of cyber-risk profiles that set out the controls and measures suppliers must meet to demonstrate sufficient mitigation of their cyber risks before they are allowed to start work on an MoD contract.

This effort to bolster the cybersecurity of the entire supply chain follows such attacks as WannaCry and Petya, which demonstrated that many companies are not resilient to a cyberattack. Businesses that are unable to validate that they have addressed the DEFSTAN 05-138 controls risk contract termination and the payment of damages.

HELPING SUPPLIERS COMPLY WITH THE UK MINISTRY OF DEFENCE'S DEFCON 658 REQUIREMENTS

DATA PROTECTION REQUIREMENTS

The DEF STAN 05-138 includes several controls specific to the protection of sensitive information, as outlined below. Thales provides data security solutions that help address these controls, as indicated. Note that while the controls are defined based on the risks associated with the contract (Low, Medium or High), Thales's solutions apply across similar controls simultaneously, and are therefore consolidated below.

Control Measure	Thales Coverage
L.07 Define and implement a policy to control access to information and information processing facilities. **M.06** Ensure the organisation has identified asset owners and asset owners control access to their assets. **L.12** Define and implement a policy to manage the access rights of user accounts.	Thales's Vormetric Data Security Platform provides state of the art user access control: **Separation of privileged access users and sensitive user data.** With the Vormetric Data Security Platform, administrators can create a strong separation of duties between privileged administrators and data owners. Vormetric Transparent Encryption encrypts files, while leaving their metadata in the clear. In this way, IT administrators—including hypervisor, cloud, storage, and server administrators—can perform their system administration tasks, without being able to gain privileged access to the sensitive data residing on the systems they manage. **Separation of administrative duties.** Strong separation-of- duties policies can be enforced to ensure one administrator does not have complete control over data security activities, encryption keys, or administration. In addition, the Vormetric Data Security Manager supports two-factor authentication for administrative access. **Granular privileged access controls.** The Vormetric platform can enforce very granular, least-privileged-user access management policies, enabling protection of data from misuse by privileged users and APT attacks. Granular privileged-user-access management policies can be applied by user, process, file type, time of day, and other parameters. Enforcement options can control not only permission to access clear-text data, but what file-system commands are available to a user.
L.10 Define and implement an information security policy, related processes and procedures. **M.04** Define and implement a policy for storing, accessing, and handling sensitive information securely.	**Detailed security policies.** The platform delivers centralized controls that enable consistent and repeatable management of encryption, access policies and security intelligence for all your structured and unstructured data. It is available as FIPS 140-2 and Common Criteria certified virtual and physical appliances. **Extensibility.** Built on an extensible infrastructure, components of the Vormetric Data Security Platform can be deployed individually, while offering efficient, centralized key and policy management. **Robust security for sensitive data.** Thales e-Security helps protect sensitive data through Vormetric Transparent Encryption with integrated Key Management for data at rest, Application Encryption, Tokenization with Dynamic Masking. These techniques make the data meaningless and worthless without the keys to decrypt it.
L.16 Define and implement an incident management policy, which must include detection, resolution and recovery.	**Security intelligence.** The Vormetric Platform provides security intelligence logs that specify which processes and users have accessed protected data, under which policies, and if access requests were allowed or denied. The management logs will even expose when a privileged user submits a command like 'switch users' in order to attempt to imitate, and potentially exploit, the credentials of another user. Sharing these logs with a security information and event management (SIEM) platform helps uncover anomalous patterns in processes and user access, which can prompt further investigation. For example, an administrator or process may suddenly access much larger volumes of data than normal, or attempt to do an unauthorized download of files. These events could point to an APT attack or malicious insider activities.
M.16 Define and implement a policy to secure organisational assets when individuals cease to be employed by your organisation.	**Privileged access controls and intelligence logs.** The Vormetric platform's granular access management policies can be applied by user and access can be revoked for individuals who have left the organisation. Any denied attempts to access sensitive data will be captured by Vormetric's security intelligence logs.

LEARN MORE

Please visit **www.thalesesecurity.com** to learn more about how we can help you comply with DEFCON 658

Follow us on:

Americas – Thales eSecurity Inc. 900 South Pine Island Road, Suite 710, Plantation, FL 33324 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