



## Use of **USB storage** devices in the DND/CAF

As part of an overall strengthening of the cybersecurity posture, DND/CAF will **significantly reduce the number of USB storage devices** on all GC/DND IT systems. At completion, authorized devices will be centrally registered and monitored while **unauthorized devices will be blocked**.

### Security requirements you need to know:

- Authorized USB devices must be centrally registered and monitored by your Information System Security Officer (ISSO).  
Data Loss Prevention tools track data transfers, ensure only approved devices connect, and flag unusual activity.
- All unregistered USB Storage will be blocked.
- There are **regular security audits**, including device logs and transfers.

USB storage devices **should only be considered** if no other options are available.

### For more information

- DND/CAF Information Technology Security Standard **ITSS-01 for Portable Information Technology Devices**
- For alternative file transfer options **JJIFC – Data Transfer Service**



To report a security incident  
or for all questions:

**DIM Secur OPS**

