IdenTrust
part of HID

Safeguarding of Sensitive and Unclassified DoD Information

Cyber theft of Department of Defense (DoD) program information from defense contractors unclassified computer networks puts the U.S. military's technological advantage at risk. Theft of information pertaining to DoD capability development can allow adversaries to bypass costly and lengthy research and development cycles and/or understand enough about U.S. military technology to develop countermeasures.

Best practices to mitigate the risk of information theft are to implement commensurate information security controls such as logical access controls, audit and accountability controls, configuration management controls, physical access controls and increasingly **controls to encrypt data at rest and in transit to protect sensitive information from theft.** It is critical that all DoD contractors implement best practice information security controls to mitigate the risk of information theft.

Recognizing the need to ensure contractors implement best practice controls, the DoD developed new policy to mitigate this risk by including new clauses in the Defense Federal Acquisition Regulation Supplement (DFARS). **The new DFARS clauses require Enhanced Safeguarding of Unclassified DoD Information** mandating the use of specific NIST SP800-53 controls.

While most of the required security controls represent best practices already in place within most contractor organizations, many contractors do not today implement controls to protect transmitted information. The new DFARS clauses specifically require the use of **cryptographic mechanisms to prevent unauthorized disclosure of information during transmission for many types of unclassified DoD information.**

DoD ECA Certificates from IdenTrust are individually issued identity credentials intended for the DoD contractor community. DoD contractors can use these credentials to:

Meet DFARS requirements for Safeguarding of Unclassified DoD Information

- Digitally sign and encrypt email or documents
- Ensure only intended recipient(s) can decrypt transmitted data
- Ensure integrity of encrypted information
- Ensure the identity of the sender of information
- Authenticate and establish your identity when accessing a protected DoD or DoD contractor system.

In addition to meeting DFARS requirements and providing authentication to DoD systems, ECA certificates provide many other benefits, including reducing risk from:

- Loss of reputation;
- Industrial espionage; and
- Failure to meet audit and compliance requirements.

IdenTrust has developed a full education program to help contractors understand how the use of IdenTrust-issued DoD ECA digital certificates will enable them to implement "Best Practice" DFARS required controls for Safeguarding of Unclassified DoD Information as well as how to achieve other benefits from the use of a DoD ECA digital certificate. To learn more about our webinars or to implement the use of DoD ECA certificates in your business, please contact: IdenTrust at ECASales@identrust.com

IdenTrust bundles each ECA identity certificate with an ECA encryption certificate, providing the following capabilities:

- Authentication into PKI-enabled DoD information systems
- Digital signing of documents and emails
- Encryption of documents and emails

2025-03-20-identrust-eca-DFARS