HIGHSIDE

CMMC Compliance

US Department of Defence Cybersecurity Maturity Model Certification

The United States Department of Defense (DoD) created the Cybersecurity Maturity Model Certification (CMMC) for contractors to reduce the theft of intellectual property. The CMMC gives the DoD a mechanism to certify the cyber readiness of defense contractors. The new CMMC provides for five levels of certification in both cybersecurity practices and processes. Contractors choose their maturity certification level based on the requirements of the projects they are or will be involved with. Failure to adhere to these new requirements will result in loss of contracts with the DoD. The CMMC is based on NIST and ISO standards, however, unlike self-attestation for NIST compliance, the CMMC requires a third party assessment for certification. Passing a CMMC assessment requires preparation.

There are three areas when dealing with Controlled Unclassified Information (CUI) that require focus. These three key functional areas are:

- People
- Process
- Technology

CMMC Requirements & Deep-Dive

The Cybersecurity Maturity Model Certification (CMMC) combines various cybersecurity standards and best practices. These controls and processes are mapped across several maturity levels. These levels range from level one, basic cyber hygiene, to level 5, advanced cybersecurity. For a given CMMC level, the associated controls and processes, when implemented correctly, will reduce risk against a specific set of cyber threats. Contractors determine which maturity level they need to be certified for based on the security level requirements of the projects they are currently working on or wish to bid on.

The CMMC effort builds upon the existing regulation (DFARS 252.204-7012) that is based on trust by adding a verification component to the cybersecurity requirements. This model is also based on best practices from existing cyber security standards such as ISO 27001, ISO 27002, ISO 27032, NIST 800-171, NIST 800-172, NIST 800-53, the UK NCSC Cyber Essentials, and the Australian ACSC Essential Eight. There are 17 capability domains with 43 capabilities, 5 processes across 5 levels, and 171 practices across five levels to measure technical capabilities. The CMMC assessment measures a contractor’s ability to safeguard Controlled Unclassified Information (CUI) and Federal Contract Information (FCI).

CMMC assessments are performed by authorized and accredited CMMC Third Party Assessment Organizations (C3PAOs). Once assessed, C3PAOs will issue CMMC certificates to Defense Industrial Base (DIB) companies at the appropriate level. CMMC certification will be a requirement for an organization doing business with the DoD. Both prime contractors and subcontractors will require certification. Assessment should be done across:

- All team members with access to program documentation (in any format, including email and attachments)
- All IT staff with privileges that could be used to gain access to program documents/data
- All service providers with privileges that could be used to gain access to documents/data or systems

It is nearly impossible to comply without significantly limiting WHO has access to WHAT information and WHERE they have access to the SYSTEMS that store and process program information

In preparation for CMMC compliance, the goal should

HighSide Simplifies CMMC Compliance

HighSide's easy to deploy technology solutions simplify the CMMC preparation and help with practices in 9 of the 17 domains.

HighSide's technologies are built on our end-to-end encryption and authentication protocol. Our approach to security helps organizations improve their security, lower their risk, and reduce their CMMC scope. The fastest way to get started on your compliance journey is to start a complimentary trial of our SecureCollab and experience for yourself a more secure way of collaboration.

Collaborate with Sensitive Data & Ensure Compliance

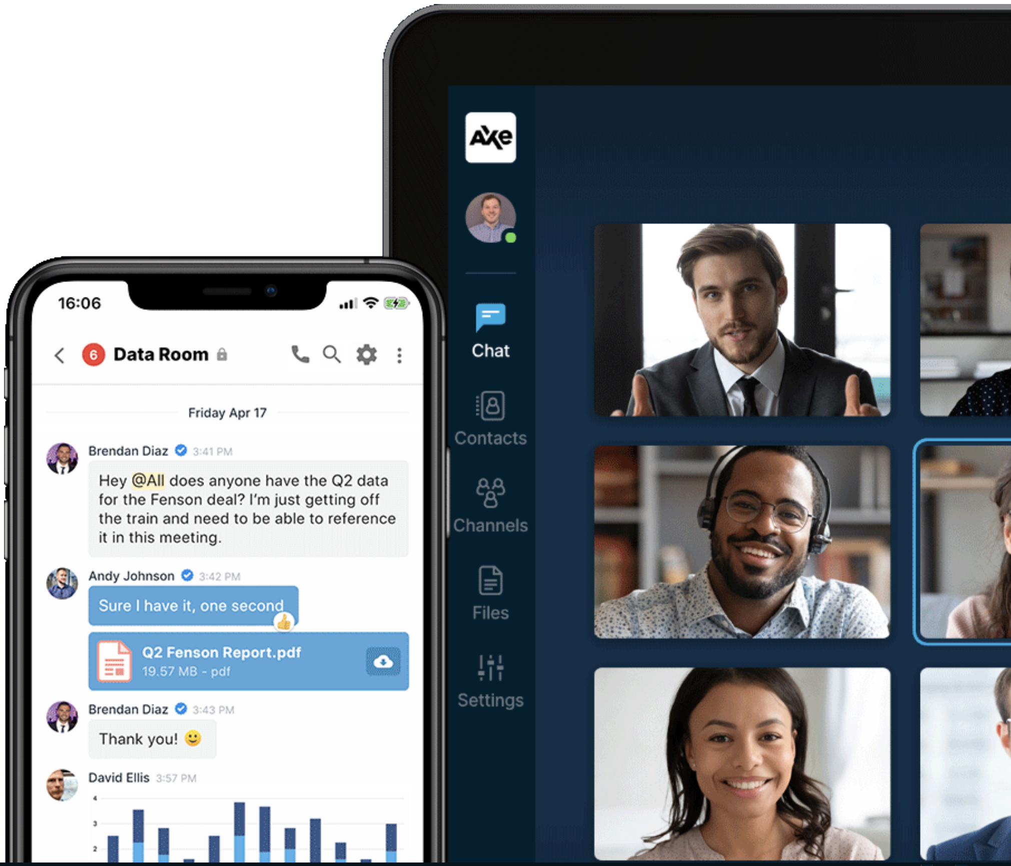
HighSide gives organizations the ability to collaborate on sensitive projects, share confidential information and meet CMMC compliance

Securely Store & Share Files in the Cloud

With HighSide's e-2-e encryption and distributed trust architecture, your data is secure at rest, safe in transit and readily available for user collaboration.

Broker Access & Authentication with Zero Trust

Guarantee only those authorized (and in authorized locations, on authorized devices, etc) can access sensitive information - and do it in a seamless manner for both administrative staff and end users.



16:06

6 Data Room

Friday Apr 17

Brendan Diaz 3:41 PM

Hey @All does anyone have the Q2 data for the Fenson deal? I'm just getting off the train and need to be able to reference it in this meeting.

Andy Johnson 3:42 PM

Sure I have it, one second

Q2 Fenson Report.pdf
19.57 MB - pdf

Brendan Diaz 3:43 PM

Thank you! 🙂

David Ellis 3:57 PM

HIGHSIDE

HighSide is the global leader in secure cloud sharing, collaboration & access management. Powered by a distributed cryptographic key management infrastructure, HighSide's suite of products enable businesses to engage securely in a remote first world. Through our zero-trust technology, teams have access to a modern unified communications and file sharing platform including voice, video, text and files, reducing risk of shadow IT and reliance on dated and insecure communications channels.

HighSide delivers applications that users actually want to use and that security leaders want to deploy. Founded in 2015, the company has offices in Columbia, MD, Esch-sur-Alzette, Luxembourg and New York, NY.

highside.io
sales@highside.io