code42

Code42's Incydr GOV and Cybersecurity Maturity Model Certification (CMMC)

CMMC - What is it and how does Incydr help its customers maintain compliance?

Incydr, our Insider Risk Management solution, supports customer compliance with Cybersecurity Maturity Model Certification (CMMC) requirements by providing organizations with end to end data encryption, log encryption, data protection, critical data control and security they need for handling Department of Defense (DoD) related Controlled Unclassified Information (CUI) and Federal Contract Information (FCI). In addition, Incydr provides powerful foundational capabilities to detect, investigate and respond to file exposure and exfiltration risks without disrupting legitimate collaboration.

What is CMMC?

In January 2020, the DoD released the Cybersecurity Maturity Model Certification (CMMC) v1.0. The CMMC model builds on the standards called for in the current DFARS rule, namely NIST Special Publication 800-171 – Protecting Controlled Unclassified Information (CUI) in Non-federal Systems and Organizations. The certification process will require companies to be audited by a Certified Third- Party Assessment Organization (C3PAO). These certifications will follow a set of standards that will ensure that the CMMC is interpreted the same way across the board.

Who does CMMC apply to?

If a Defense Industrial Base (DIB) Contractor provides services to the federal government— specifically the Department of Defense (DoD) —the Cybersecurity Maturity Model Certification (CMMC) applies to them. In fact, every DoD contractor who handles DoD's Controlled Unclassified Information (CUI) and Federal Contract Information (FCI) will be required to comply with DoD's CMMC certification process. If the organization does not get the certification, it may be ineligible to bid on or perform government work.

How does Incydr Gov help its customers maintain CMMC compliance and contractual requirements to the DoD?

Our Incydr product delivers several key functionalities that play a vital role in supporting CMMC:

- End-to-end encryption: Customer file data, including event, alert, and audit log data, is encrypted with end-to-end encryption using AES 256-bit FIPS 140-2 validated modules to secure data at rest and AES 256-bit Transport Layer Security (TLS 1.2) encryption to secure all data in transit.
- Insider Risk Management - Inside Risk Indicators: CMMC requires organizations to incorporate into security training and awareness the ability to recognize and report potential indicators on insider risk. With Incydr you get real-time visibility into data exfiltration events and actionable insight into Insider Risk Indicators within your organization.
- Cloud Based Services: The Incydr product collects exfiltrated endpoint data to allow for recovery and restoration of data for investigations. This data is retained for 30 or 90 days, depending on the subscription purchased.
- Transparency and Accountability: The Incydr product captures and retains user data movement, so a user's actions are logged and can be reviewed for malicious data exfiltration events.

CMMC Highlights

Does Incydr align with CMMC and NIST 800-171?
Incydr has performed an internal control self-assessment and meets the criteria for NIST SP 800-171. Code42 is also self- assessed at CMMC Level 3 Good Cyber Hygiene. Incydr has performed a self-assessment of the CMMC capabilities.

How do you know what level of CMMC you will need?
The level a CSP needs depends on the type of information it handles, and the requirement set forth in the Government contract or subcontract. CMMC divides information into two big "buckets":

- Federal Contract Information ("FCI") is "information provided by or generated for the Government under contract not intended for public release".
- Controlled Unclassified Information ("CUI" is "information that requires safeguarding or dissemination controls pursuant to and consistent with laws, regulations, and government wide policies," but is not classified. CUI generally includes things like personally identifying information, Government financial records, and controlled technical information.

What CMMC level is required from companies?

The DoD has made it clear that all companies doing business with the DoD will need to be at minimum, Level 1 certified. If CUI and FCI is processed Level 3 is required.

How long is the CMMC certification valid?

3 years

Incydr Highlights

- Monitors ALL exfiltrated file movement - including CUI, FCI and other sensitive data
- Provides the capability to Detect, Investigate and Respond to file exposure and exfiltration including web browser uploads, cloud sync activity, file sharing, Airdrop, and use of removable media.

Incydr CMMC Self-Assessment Level

Incydr has completed a detailed self-assessment of CMMC including practices and processes. Based on this, Incydr aligns with the requirements of CMMC Level 3 which focuses on the protection of CUI and FCI and encompasses in NIST SP 800-171 Rev. 2 and DFARS Clause 252.204.7012. Additionally, Incydr aligns with the subset of enhanced security requirements from draft NIST 800-171B as well as other Cybersecurity best practices. These practices enhance the detection and response capabilities of an organization's Incident Response capabilities and to address and adapt to the changing tactics, techniques and procedures (TTP's) used by APT's.

Level 1

BASIC CYBER HYGIENE

17 PRACTICES

- ✓ Equivalent to all practices in Federal Acquisition Regulation (FAR) 48 CFR 52.204-21

Level 2

INTERMEDIATE CYBER HYGIENE

72 PRACTICES

- ✓ Comply with the FAR
- ✓ Includes a select subset of 48 practices from the NIST SP 800-171 r1
- ✓ Includes an additional 7 practices to support intermediate cyber hygiene

Level 3

GOOD CYBER HYGIENE

130 PRACTICES

- ✓ Comply with the FAR
- ✓ Encompasses all practices from NIST SP 800-171 r1
- ✓ Includes an additional 20 practices to support good cyber hygiene

Level 4

PROACTIVE

156 PRACTICES

- ✓ Comply with the FAR
- ✓ Encompasses all practices from NIST SP 800-171 r1
- ✓ Includes a select subset of 11 practices from Draft NIST SP 800-171B
- ✓ Includes an additional 15 practices to demonstrate a proactive cybersecurity program

Level 5

ADVANCED / PROGRESSIVE

171 PRACTICES

- ✓ Comply with the FAR
- ✓ Encompasses all practices from NIST SP 800-171 r1
- ✓ Includes a select subset of 4 practices from Draft NIST SP 800-171B
- ✓ Includes an additional 11 practices to demonstrate an advanced cybersecurity program

* https://www.acq.osd.mil/cmmc/

Gartner Peer Insights

35+ Verified Security Reviews

★★★★★

4.9 out of 5 stars

About Code42

Code42 is the leader in Insider Risk Management. Native to the cloud, the Code42® Incydr™ solution rapidly detects data loss and speeds incident response without inhibiting employee productivity. With Code42, security professionals can protect corporate data and reduce insider threats while fostering an open and collaborative culture for employees. More than 50,000 organizations worldwide, including the most recognized brands in business and education, rely on Code42 to safeguard their ideas. For more information, visit **code42.com**.