CODE42

TECH OVERVIEW

CODE42'S INCYDR GOV AND CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)

CMMC Highlights

Does Incydr Gov align with CMMC and NIST 800-171?
Code42 has performed an internal control self-assessment for its Incydr Gov product and meets the criteria for NIST SP 800-171.

Incydr Gov is also self-assessed at CMMC Level 3 Good Cyber Hygiene. Code42 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

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

Incydr Gov, Code42's Federal Insider Risk Detection and Response solution supports customer compliance with Cybersecurity Maturity Model Certification (CMMC) requirements, by providing organizations with end to end data encryption, log encryption, data preservation, 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, Code42 Incydr Gov provides a powerful foundational capabilities to detect, investigate and respond to effectively mitigate file exposure and exfiltration risks without disrupting legitimate collaboration.

What is CMCC?

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 Revision 1 – 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?

Code42 Incydr Gov endpoint data protection delivers several key functionalities that play a vital role in supporting CMMC:

- **End-to-end encryption**
  All federal customer file data, including event, alert, and audit log data, is encrypted with end-to-end encryption using AES 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 and Inside Risk Indicators**
  CMMC requires companies to incorporate into security training and awareness recognizing and reporting potential indicators on insider risk. With Incydr Gov, customers get real-time visibility into data exfiltration events and actionable insight into insider risk indicators within your organization.
- **Cloud Based Services** -
  Code42's Incydr Gov product preserves customer endpoint data to allow for recovery and restore of data for investigations. It also identify files that are shared externally via corporate OneDrive, Google Drive and Box accounts.
- **Security and Privacy Protocols**
  Incydr Gov provides encryption key escrow, with strict controls around key access.
- **Transparency and Accountability**
  Incydr Gov captures and retains user data movement, so a user's actions are logged and can be reviewed for malicious data ex-filtration events.

Incydr Gov Highlights

- Monitors ALL 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.

Code42 Incydr Gov CMMC Self-Assessment Level

Code42 has completed a detailed self-assessment of CMMC including practices and processes. Based on this, Incydr Gov 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 Gov 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 organizations Incident Response capabilities and to address and adapt to the changing tactics, techniques and procedures (TTP's) used by APT's.

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

CODE42

Corporate Headquarters
100 Washington Avenue South
Minneapolis, MN 55401
612.333.4242
code42.com

Code42 is the leader in insider risk detection and response. Native to the cloud, Code42 rapidly detects data loss, leak, theft and sabotage as well as speeds incident response – all without lengthy deployments, complex policy management or blocking employee productivity. With Code42, security professionals can protect corporate data and reduce insider risk while fostering an open and collaborative culture for employees. Backed by security best practices and control requirements, Code42's insider risk solution can be configured for GDPR, HIPAA, PCI and other regulatory frameworks.

More than 50,000 organizations worldwide, including the most recognized brands in business and education, rely on Code42 to safeguard their ideas. Founded in 2001, the company is headquartered in Minneapolis, Minnesota, and backed by Accel Partners, JMI Equity, NEA and Split Rock Partners. Code42 was recognized by Inc. magazine as one of America's best workplaces in 2020. For more information, visit code42.com, read Code42's blog or follow the company on Twitter. (WP2103247)