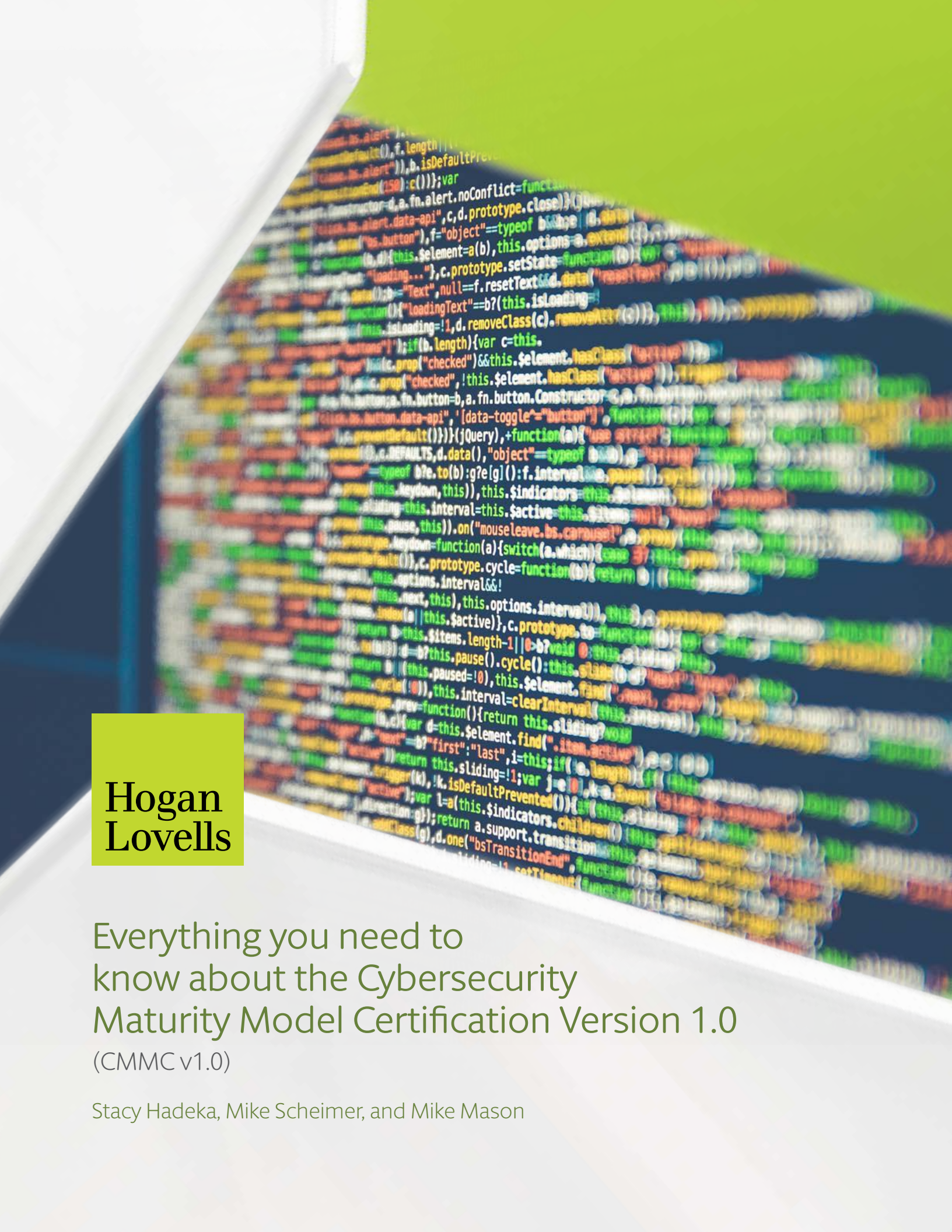


Hogan Lovells

Everything you need to know about the Cybersecurity Maturity Model Certification Version 1.0

(CMMC v1.0)

Stacy Hadeka, Mike Scheimer, and Mike Mason

What is CMMC?

CMMC is a unified cybersecurity standard and certification program for **all** U.S. Department of Defense (DoD) contractors. On January 31, 2020, DoD's Office of the Under Secretary of Defense for Acquisition & Sustainment (OUSD(A&S)) released CMMC v1.0. DoD intends to continuously update the model to adjust to evolving threats.

Who is subject to CMMC?

All U.S. DoD contractors and subcontractors, including commercial item contractors, are subject to CMMC. Currently the model is limited to DoD-only, but may be adopted by other U.S. civilian agencies in the future.

Is compliance with current DoD cybersecurity standards enough?

No, CMMC is a new standard that builds upon and goes beyond the current DoD requirements such as National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, and DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. CMMC combines various standards, including NIST SP 800-171, NIST SP 800-171B, NIST SP 800-53, and others.

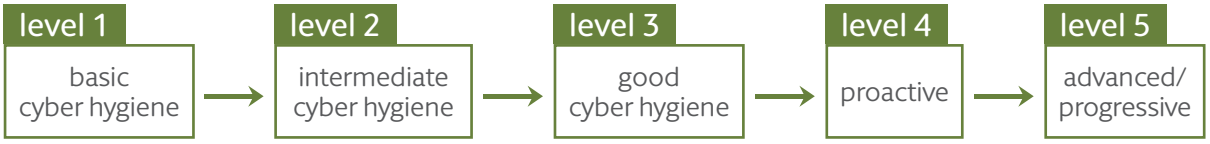
What are the model's key features?

CMMC measures cybersecurity maturity with 5 **levels** that align a set of 5 maturity **processes** and 171 cybersecurity best **practices** with the type of information to be protected and the associated range of threats. These 5 processes and 171 practices are organized into a set of 17 **domains**. The 171 practices are also aligned to a set of 43 **capabilities** within each domain.

The CMMC levels and the associated sets of processes and practices across domains are cumulative. In order to achieve a specific level, a contractor must also demonstrate achievement of any preceding lower level(s).

Levels:

The 5 levels measure cybersecurity maturity



Domains:

The 17 domains are sets of capabilities that are based on cybersecurity best practices. Each domain is assessed for practice and process maturity across the 5 defined levels. In addition to the security families from NIST publications, CMMC includes its own unique domains, including Asset Management (AM), Recovery (RE), and Situational Awareness (SA).

Capabilities:

The 43 capabilities are achievements to ensure cybersecurity objectives are met within each domain, e.g., each domain is comprised of a set of capabilities. Capabilities are met through the employment of practices and processes.

Processes:

The 5 processes measure a contractor's process maturity (i.e., institutionalization) spanning Maturity Levels 2-4:

CMMC maturity level	Maturity level description	Processes
Level 1	Performed	*There are no maturity processes assessed at Maturity Level 1. An organization performs Level 1 practices but does not have process institutionalization requirements.*
Level 2	Documented	Establish a policy that includes [DOMAIN NAME]. Document the CMMC practices to implement the [DOMAIN NAME] policy.
Level 3	Managed	Establish, maintain, and resource a plan that includes [DOMAIN NAME].
Level 4	Reviewed	Review and measure [DOMAIN NAME] activities for effectiveness.
Level 5	Optimizing	Standardize and optimize a documented approach for [DOMAIN NAME] across all applicable organization units.

Process institutionalization provides additional assurances that the practices associated with each level are implemented effectively.

Practices:

The 171 cybersecurity best practices measure a contractor's technical capabilities. They are derived from multiple cybersecurity standards, frameworks, and other references.

CMMC maturity level	Focus	Practices	Total accumulated practices
Level 1	Safeguard Federal Contract Information (FCI)[1]	17[2]	17
Level 2	Serve as transition step in cybersecuity maturity progression to protect Controlled Unclassified Information (CUI)[3]	55	72
Level 3	Protect CUI	58	130
Level 4	Protect CUI and reduce risk of Advanced Persistent Threats (APTs)	26	156
Level 5	Protect CUI and reduce risk of Advanced Persistent Threats (APTs)	15	171

1. FCI is information provided by or generated for the Government under contract not intended for public release.
2. The 15 safeguarding requirements from FAR 52.204-21 correspond to 17 security requirements from NIST 800-171, and in turn, 17 practices in CMMC.
3. CUI is information that requires safeguarding or dissemination controls pursuant to and consistent with the law, regulations, and government-wide policies, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended.

How do the practices map to current standards?

Level 1 is equivalent to all of the safeguarding requirements from FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems.

Level 2 serves as a progression from Level 1 to Level 3 and consists of a subset of the security requirements specified in NIST SP 800-171, as well as 7 practices from other standards and references.

Level 3 includes all of the security requirements in NIST SP 800-171, plus 20 other practices.

Levels 4-5 include all of the security requirements in NIST SP 800-171 plus a subset of the enhanced security requirements from Draft NIST SP 800-171B, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations: Enhanced Security Requirements for Critical Programs and High Value Assets.

In addition to NIST SP 800-171 and 800-171B standards, CMMC includes practices from additional sources, such as the UK Cyber Essentials and Australia Cyber Security Centre Essential Eight Maturity Model.

Can I self-attest my compliance?

No, a trained and licensed Assessor from a Certified Third-Party Assessment Organization (C3PAO), which in turn is certified by the CMMC Accreditation Body (CMMC-AB), must certify your compliance.

- CMMC-AB: A not-for-profit organization that will establish and oversee a community of C3PAOs and Assessors that will assess participating organizations against CMMC's unified cybersecurity standard. The CMMC-AB will sign a Memorandum of Understanding (MOU) with DoD outlining the roles, rules, and responsibilities for training and licensing C3PAOs and Assessors.
- C3PAO: An entity that must be licensed by the CMMC-AB and will house at least two Assessors.
- Assessors: Responsible for auditing over 300,000 contractors. Assessors will receive a license from the CMMC-AB after completing required training. Assessors will not work for the CMMC-AB but will work for C3PAOs.
- Trainers: In order to field a cadre of 10,000 or more professional Assessors, the trainers will educate and ensure that the CMMC framework is uniformly applied through standardized Assessor training.

How will CMMC be implemented?

DoD will roll out CMMC in a phased approach over the next 5 years. CMMC is solely limited to future work – it will not impact existing contracts nor will it apply retroactively. DoD will identify the required CMMC level in Request for Proposal (RFP) Sections L and M and use as a "go / no go decision."

DoD intends to include the new CMMC requirements in 10 "pathfinder programs." An initial 10 Requests for Information (RFIs) with CMMC requirements will be issued in June 2020 and 10 RFPs will be released in October 2020, with each contract expected to involve up to 150 subcontractors. These RFIs/ RFPs will contain a mix of CMMC levels.

DoD expects the number of contracts with CMMC requirements to reach 75 by Fiscal Year (FY) 2022, 250 contracts by FY 2023, and 479 contracts in FY 2024. DoD expects all new DoD contracts to contain CMMC requirements starting in FY 2026. DoD also expects to have 1,500 contractors certified in FY 2021, 7,500 more in FY 2022, 25,000 more by FY 2023, and almost 48,000 by FY 2025.

DoD will issue a proposed DFARS rule in Spring 2020 that will implement CMMC through regulation. See DFARS Case 2019-D041, Strategic Assessment and Certification Cybersecurity Requirements.

How will a contractor be certified?

A contractor will coordinate with a C3PAO and Assessor to request and schedule a CMMC assessment. A contractor will specify the level of the certification requested based on its specific business requirements. A contractor will be certified at the appropriate CMMC level upon demonstrating the appropriate maturity in practices and processes to the satisfaction of the Assessor. DoD expects there to be some level of reciprocity or credit for previous cybersecurity audits or certifications from the government.

A CMMC certification must be obtained at the time of contract award and will be effective for 3 years. DoD is in the process of creating a database that will house all contractor certifications and will be linked to a contractor's System for Award Management (SAM) account.

Subcontractors will only need to be certified to the appropriate level based on the data that they receive or develop and the work they will perform on a contract. Thus, depending on the type of work being flowed down, it is possible that a Level 3 procurement could have Level 1 subcontractors. At a minimum, all contractors and subcontractors planning to work with DoD must be certified at a Level 1.

Does the framework apply to a contractor's entire enterprise?

A contractor can achieve a specific CMMC level for its entire enterprise network or for particular segment(s) or enclave(s), depending upon where the information in need of protection is handled and stored.

Can contractors recover their costs for compliance?

DoD has indicated that CMMC certifications will be an allowable cost, but the exact method for cost recovery has yet to be determined.

Key takeaways and recommendations

1. Read the standard, assessment guidance, and training materials as they become available on https://www.acq.osd.mil/cmmc/index.html.
2. Contractors should take steps to assess their internal cyber posture and available resources, such as:
    - Identify key stakeholders
        - Consider personnel in, among others, legal, contracts, information security, training, compliance, audit, supply chain, and relevant lines of business.
    - Inventory business systems where FCI and/or CUI reside
        - Knowing where FCI and CUI is stored will help a contractor identify whether CMMC should apply to a contractor's entire enterprise network or particular segment(s) or enclave(s).
    - Assess your current NIST SP 800-171 compliance posture
        - Contractors that are new to NIST SP 800-171 and expect to host CUI should take steps to implement the NIST standards and 20 additional CMMC requirements at Level 3. Contractors already implementing NIST SP 800-171 should review their existing System Security Plans (SSPs) and Plans of Action and Milestones (POAMs) and continue to take measures to become fully compliant.
    - Establish processes and procedures for implementing CMMC
        - Assessors will be looking at the extent to which a process and practice is embedded or ingrained in the operations of a contractor. Contractors should demonstrate institutionalization of processes and practices through the creation of policies and procedures that document practices, planning activities (e.g., mission goals, project planning, etc.), standards of review and measurement, and approach to standardization.
    - Develop and institute training
        - Training is essential to educate contractor personnel about cybersecurity and keep them up-to-date on evolving standards and threats. At a minimum, contractors should consider providing annual cybersecurity training for employees who handle or mark FCI and/or CUI.
    - Consider a self-assessment or third-party audit before your formal CMMC assessment
        - Contractors should audit their security practices and processes regularly to identify any gaps, test their effectiveness, and ensure accountability. This will also help contractors prepackage materials relevant to their CMMC assessments.
3. Subscribe to the CMMC-AB listserv at https://www.cmmcab.org/ to receive newsletters on CMMC progress and take surveys seeking input from stakeholders.
4. If you are a small business, connect with your local Procurement Technical Assistance Center (PTAC), as DoD is working with PTACs to help small businesses prepare for CMMC.
5. Continue to follow regulatory requirements, such as incident reporting, contained in DFARS 252.204-7012. Also monitor for any proposed update(s) to existing regulations.

CMMC Levels 2 and 3 practices beyond NIST 800-171

Capability	Level 1	Level 2	Level 3
C005 identify and document assets			**AM.3.036** Define procedures for the handling of CUI data. • CMMC [Source]
C008 perform auditing			**AU.3.048** Collect audit information (e.g., logs) into one or more central repositories. • CMMC • CIS Controls v7.1 6.5 • CERT RMM v1.2 COMP:SG3.SP1 • NIST SP 800-53 Rev 4 AU-6(4)
C010 review and manage audit logs		**AU.2.044** Review audit logs. • CMMC • CIS Controls v7.1 6.7 • NIST CSF v1.1 PR.PT-1 • CERT RMM v1.2 COMP:SG3.SP1 • NIST SP 800-53 Rev 4 AU-6	
C017 detect and report events		**IR.2.093** Detect and report events. • CIS Controls v7.1 19.4 • NIST CSF v1.1 DE.CM-1, DE.CM-2, DE.CM-3, RS.CO-2 • CERT RMM v1.2 IMC:SG2.SP1 • NIST SP 800-53 Rev 4 IR-6 **IR.2.094** Analyze and triage events to support event resolution and incident declaration. • CERT RMM v1.2 IMC:SG2.SP4 • NIST SP 800-53 Rev 4 IR-4(3)	
C018 develop and implement a response to a declared incident		**IR.2.096** Develop and implement responses to declared incidents according to pre-defined procedures. • CIS Controls v7.1 19.1 • NIST CSF v1.1 RS.RP-1 • CERT RMM v1.2 IMC:SG4.SP2 • NIST SP 800-53 Rev 4 IR-4	
C019 perform post incident reviews		**IR.2.097** Perform root cause analysis on incidents to determine underlying causes. • NIST CSF v1.1 DE.AE-2 • CERT RMM v1.2 IMC:SG5.SP1 • NIST SP 800-53 Rev 4 AU-2	
C029 manage backups		**RE.2.137** Regularly perform and test data backups. • CIS Controls v7.1 10.1, 10.3 • NIST CSF v1.1 PR.IP-4 • CERT RMM v1.2 KIM:SG6.SP1 • NIST 800-53 Rev 4 CP-9 • AU ACSC Essential Eigh	**RE.3.139** Regularly perform complete, comprehensive, and resilient data backups as organizationally defined. • CIS Controls v7.1 10.1, 10.2, 10.5 • CERT RMM v1.2 KIM:SG6.SP1 • NIST 800-53 Rev 4 CP-9, CP-9(3)
C031 identify and evaluate risk			**RE.3.144** Periodically perform risk assessments to identify and prioritize risks according to the defined risk categories, risk sources, and risk measurement criteria. • NIST CSF v1.1 ID.RA-5 • CERT RMM v1.2 RISK:SG3, RISK:SG4.SP3 • NIST SP 800-53 Rev 4 RA-3

Capability	Level 1	Level 2	Level 3
C032 manage risk			**RM.3.146** Develop and implement risk mitigation plans. • NIST CSF v1.1 ID.RA-6, ID.RM-1 • CERT RMM v1.2 RISK:SG5.SP1 • NIST SP 800-53 Rev 4 PM-9 **RM.3.147** Manage non-vendor- supported products (e.g., end of life) separately and restrict as necessary to reduce risk. • CMMC • CIS Controls v7.1 2.2 • NIST SP 800-53 Rev 4 SA-22(1)
C036 perform code reviews			**CA.3.162** Employ a security assessment of enterprise software that has been developed internally, for internal use, and that has been organizationally defined as an area of risk. • CMMC • CIS Controls v7.1 18.1, 18.2
C037 implement threat monitoring			**SA.3.169** Receive and respond to cyber threat intelligence from information sharing forums and sources and communicate to stakeholders. • CMMC • NIST CSF v1.1 ID.RA-2 • NIST SP 800-53 Rev 4 PM-16
C038 define security requirements for systems and communications		**SC.2.179** Use encrypted sessions for the management of network devices. • CMMC • CIS Controls v7.1 11.5	
C039 control communications at system boundaries			**SC.3.192** Implement Domain Name System (DNS) filtering services. • CMMC • CIS Controls v7.1 7.7 • NIST SP 800-53 Rev 4 SC-20
C042 performance network and system monitoring			**SI.3.218** Employ spam protection mechanisms at information system access entry and exit points. • CMMC • NIST SP 800-53 Rev 4 SI-8
C044 implement advanced email protections			**SI.3.219** Implement email forgery protections. • CMMC • CIS Controls v7.1 7.8 • NIST CSF v1.1 PR.DS-2 • CERT RMM v1.2 KIM:SG4.SP1 • NIST SP 800-53 Rev 4 SC-8 **SI.3.220** Utilize sandboxing to detect or block potentially malicious email. • CIS Controls v7.1 7.10 • NIST SP 800-53 Rev 4 SC-44

Alicante
Amsterdam
Baltimore
Beijing
Birmingham
Boston
Brussels
Budapest*
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta*
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Riyadh*
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ*
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar*
Warsaw
Washington, D.C.
Zagreb*

*Our associated offices
Legal Services Center: Berlin

Stacy Hadeka
Senior Associate | Washington, D.C.
T +1 202 637 3678
E: stacy.hadeka@hoganlovells.com

Mike Scheimer
Senior Associate | Washington, D.C.
T +1 202 637 6584
E: michael.scheimer@hoganlovells.com

Mike Mason
Partner | Washington, D.C.
T +1 202 637 5499
E: mike.mason@hoganlovells.com

www.hoganlovells.com