CMMC/DFARS 7012 Security Assessment

Prepared by BL King Consulting for <<Your Company>>

<<Your Company>> Security Assessment

- Reviewed and assessed <<Your Company>> IT infrastructure for compliance with NIST 800-171 from both the DFARS 7012 and CMMC viewpoint.
- Information contained within is meant to be informational and must not be construed as a CMMC Certification.
- 3rd Party Auditors may interpret requirements and implementation details differently and as a result there may be non-compliant controls (or compliant) that differ from this assessment.

Bottom Line Up Front

- Control Compliance
  - 130 Total Controls
  - 70 Non-Compliant Controls
- Additional Recurring Costs for Software & Services
  - ** / year
  - Allowable Costs for DoD Contracts
- One-Time costs
  - Hardware **
  - Documentation **
- DFARS 252.204-7012 already required on DoD contracts.
- CMMC likely not a requirement until 2022 and beyond

** Contact us for pricing: info@blking.net or 978-688-1739

Major Changes

- Recurring Security Support
- Office Building Access Control Logs
- Additional Software
- Removal of Admin Privileges from Users
- Dual Admin/User Accounts on G Suite
- Account Lockout
- Configuration Control of Hardware and Software
- Security Awareness Training
- Marking and Handling of FCI/CUI
- Single Sign On via G Suite w/ Procore to enable 2 Step Verification

Definitions

- **DFARS 252.204-7012:** Defense Federal Acquisition Regulation Supplement Regulation that requires self attestation and adherence to National Institution for Science and Technology (NIST) Special Publication (SP) 800-171.
- **NIST SP 800-171:** Security control catalog that details basic cybersecurity hygiene and basic cybersecurity requirements for Non-Federal Systems. Controls are based on NIST SP 800-53 control catalog for Federal Information Systems.
- **Cybersecurity Maturity Model Certification:** Certification process that uses Third Party Audit Organizations (3PAO) in lieu of the self attestation as well as introducing additional security controls not included in the NIST SP 800-171.

Definitions

- **Federal Contract Information:** Information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public Web sites) or simple transactional information, such as necessary to process payments.
- **Controlled Unclassified Information:** Information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended.

Applicability

- The recommended security requirements contained in NIST 800-171 are only applicable to a non-federal systems, or organizations, when mandated by a federal agency in a contract, grant, or other agreement. The requirements apply only to the components of nonfederal systems that **process, store, or transmit CUI**, or that provide security protection for such components.

- NIST 800-171 is only applicable when DFARS 252.204-7012 is included as a requirement on a contract; look in either the FAR clause section or in the DD-254

- CMMC is only applicable when it is explicitly called out as a requirement in Section L or Section M of a contract and will be a go/no-go source selection criteria. Therefore, to be able to compete on contracts that include **CUI** a company must be certified to Level 3 of CMMC.

- When NIST 800-171 was first released, FCI was included as part of the CUI definition. It has since been removed. Now FCI stands on its own and is a requirement of CMMC level 1

Differences

- DFARS has requirements that are not in NIST SP 800-171 or CMMC
  - Reporting Requirement(s)
  - Malicious Software must be delivered to DoD Cyber Crime Center (DC3)
  - Media preservation and protection -- all Disks associated with a breach must be saved/imaged for forensic analysis
  - Allow DoD to access additional information for forensic analysis
  - Damage assessments
- CMMC has 20 level 1/2/3 controls that are not included in NIST 800-171

Policies to Cover Security Gaps

- IT Access Control Policy
- IT Configuration Management Policy
- IT Identification and Authentication Policy
- IT Maintenance Policy
- IT Media Protection Policy
- IT Risk Management Policy
- IT Network and Telecommunications Policy
- IT Sensitive Data Handling Policy
- Compliant Controls should be governed by policies as well, includes ~ 5 additional policies.

Procedures to be developed

Note: Included in a System Security Plan or other procedural document as it best fits.

- Remove Administrator Permissions from General Users
- Configure Machines to Capture Relevant Audit Logging
- Enable Account Lockout after 5 Failed Attempts
- Enable Daily Session Termination for all G Suite Users
- Enable Audit log Retention, Protection, Monitoring, Reduction, and Report Generation
- Establish Configuration Management Procedures
- Disable Accounts After 30 Days of Inactivity
- Configure Minimum Password Complexity

Procedures to be developed

- Account Generation Procedure
- Incident Response Procedures
- CUI Handling Procedures That Cover:
- Risk Management Procedures

Additional Software Requirements

- Recurring Software (Cloud or On-Premise)
  - Remote Management and Maintenance
  - Security Information and Event Management
  - Vulnerability Scanning
  - Security Awareness Training

Contact us for pricing: info@blking.net or 978-688-1739

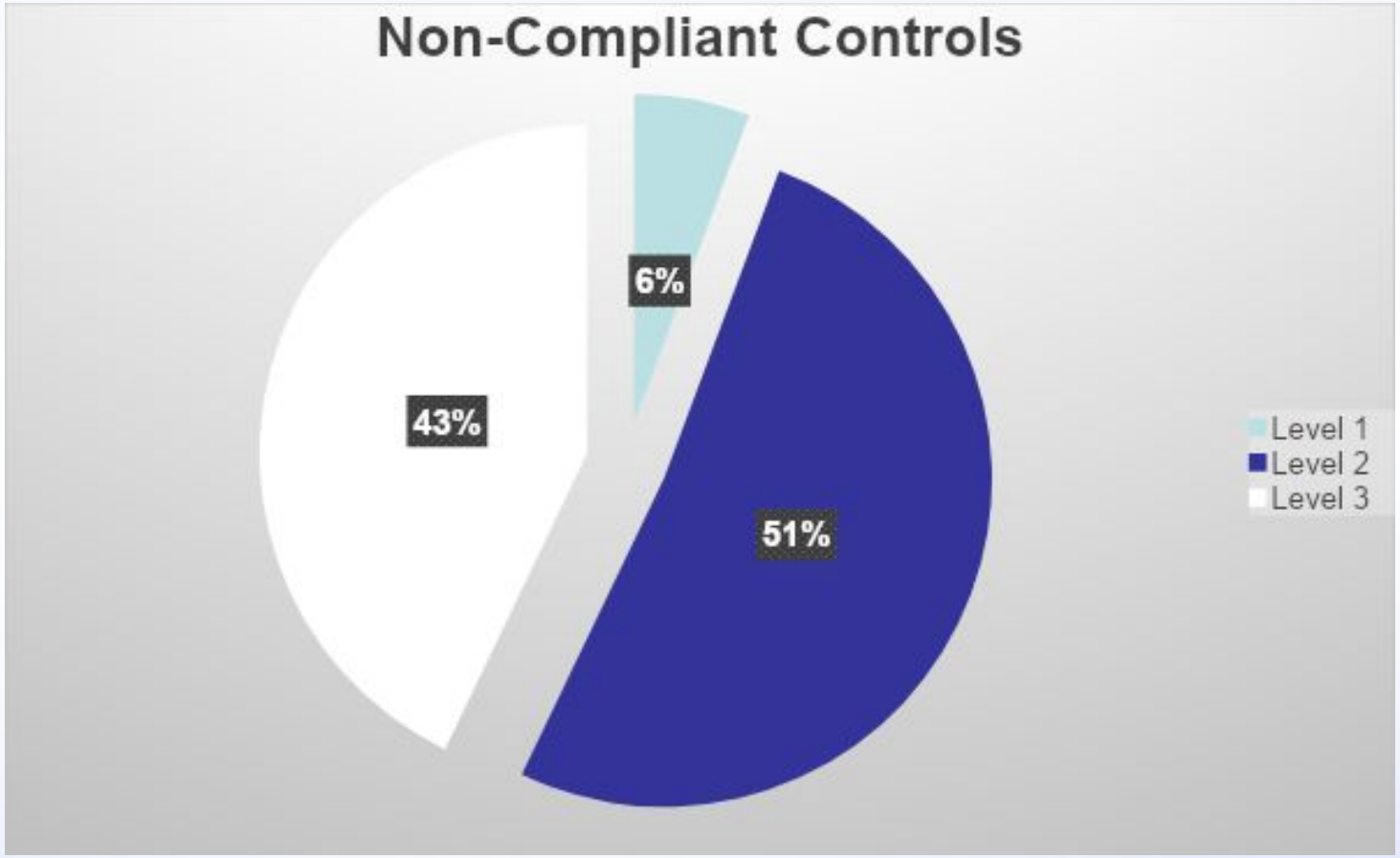
Additional Services

- Recurring Services
  - System Configuration
  - Incident Response
  - Patch Management
  - Audit Log (SIEM) Monitoring
  - Vulnerability Scanning / Remediation
  - Continuous Monitoring and Risk Management
- One-Time Services
  - Development of System Security Plan and Procedures
  - Development of IT Security Policies

Contact us for pricing: info@blking.net or 978-688-1739

Non-Compliant Controls

- 130 Total Controls
- 70 Non-Compliant
  - 4 Level 1
  - 36 Level 2
  - 30 Level 3



Non-Compliant Level 1 Controls

- Sanitize or destroy information system media containing CUI before disposal or release for reuse.
- Escort visitors and monitor visitor activity.
- Maintain audit logs of physical access.
- Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.