Managed Compliance Service
CMMC Compliance for DOD Contractors
• The FAR Clause 52.204-21 established safeguarding requirements for systems where federal contract information may reside or through which it may flow

• Imposes 15 basic security controls on systems
  – Eg. Access Control, Identification and Authentication, Physical Security

• The FAR requirements are immediately effective when a contract is awarded that contains the clause

• Flow down to sub-contractors
• The DFARS Clause 252.204-7012 established a requirement for “adequate security” for the information (differs based on the type of data)
  – Covered Defense Information (CDI)
  – Controlled Technical Information
  – Critical Information
  – Export Control Information
  – Other information identified in the contract

• The DFARS clause has flow-down requirements and requires incident reporting to both the government and the Prime contractor

• The DFARS clause also grants DoD personnel access to the contractor’s system to investigate the incident
• Under the DFARS provisions, contractors were directed to implement NIST 800-171 standards “as soon as practical, but not later than December 31, 2017.”

• Contractors must notify the DoD CIO, within 30 days of award, of any NIST 800-171 security requirement that has not been implemented at the time of contract award.

• The DFARS clause has specific requirements for incident reporting within 72 hours.
DFARS Compliance Requirements

- Assess against 110 controls defined in NIST SP 800-171
- Document compliance status with respect to each requirement
- Document areas of non-compliance and remediation plans (POA&M)
- Be prepared for audits and/or requests for compliance attestation / reports (reporting and audit mechanisms not yet clear)
- Implement breach reporting requirements (within 72 hours)
The **Cybersecurity Maturity Model Certification (CMMC) framework** was launched to further enhance the protection of sensitive information relating to contractor services provided to the DoD. Sensitive information includes:

- **Federal Contract Information (FCI)** - Information not intended for public release. It is provided by or generated for the government under a contract to develop or deliver a product or service to the Government. FCI does not include information provided by the Government to the public.

- **Controlled Unclassified Information (CUI)** - Information the government creates or possesses, or that an entity creates or possesses for or on behalf of the government, that a law, regulation, or government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.
CMMC REQUIREMENTS FOR CONTRACTORS

Additional types of CUI data include:

- **Controlled Technical Information (CTI)** – Technical information with military or space application that is subject to controls on its access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.

- **Covered Defense Information (CDI)** – Defined in DFARS 252.204-7012 as unclassified CTI or other information, as described in the CUI registry that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and government-wide policies.
CMMC REQUIREMENTS FOR CONTRACTORS

The CMMC framework implements a tiered approach to audit contractor compliance with NIST SP 800-171, based on five different levels of maturity expectations. The CMMC includes 17 capability domains, 43 capabilities, 5 processes across five levels to measure process maturity and 171 practices across five levels to measure technical capability.

- **Level 1** – Basic Cyber Hygiene: Requires 17 controls. Level 1 will likely be required of all contractors doing business with the DoD, with select practices being documented where required. Appropriate for smaller contractors that only handle FCI.

- **Level 2** – Intermediate Cyber Hygiene: Requires 72 controls. Level 2 is designed to be a bridge to Level 3 compliance, where contractors get into the practice of documenting each practice involving CUI.
CMMC REQUIREMENTS FOR CONTRACTORS

- **Level 3** – Good Cyber Hygiene: Requires 130 controls. Level 3 is a managed state where a policy has been put into place and maintained to cover all activities, with all CUI practices documented.

- **Level 4** – Proactive Cybersecurity: Requires 156 controls. Level 4 requires the implementation of more advanced security practices based largely on the NIST 800-171B, where activities are reviewed and measured for effectiveness.

- **Level 5** – Advanced/Progressive Cybersecurity: Requires 171 controls. Level 5 is the optimized state requiring highly advanced cybersecurity practices with a tested, standardized, and documented approach seen across all applicable organizational units.
## CMMC Requirements for Contractors

<table>
<thead>
<tr>
<th>Domain</th>
<th>Capabilities</th>
<th>Total Practices per Domain</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
<th>Level 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td>4</td>
<td>26</td>
<td>4</td>
<td>10</td>
<td>8</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>Asser Management</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Audit and Accountability</td>
<td>4</td>
<td>14</td>
<td>0</td>
<td>4</td>
<td>7</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Awareness and Training</td>
<td>2</td>
<td>5</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Configuration Management</td>
<td>2</td>
<td>11</td>
<td>0</td>
<td>6</td>
<td>3</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Identity and Authorization</td>
<td>1</td>
<td>11</td>
<td>2</td>
<td>5</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Incident Response</td>
<td>5</td>
<td>13</td>
<td>0</td>
<td>5</td>
<td>2</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Maintenance</td>
<td>1</td>
<td>6</td>
<td>0</td>
<td>4</td>
<td>2</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Media Protection</td>
<td>4</td>
<td>8</td>
<td>1</td>
<td>3</td>
<td>4</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Personnel Protection</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Physical Protection</td>
<td>1</td>
<td>6</td>
<td>4</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Recovery</td>
<td>1</td>
<td>4</td>
<td>0</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>Risk Management</td>
<td>2</td>
<td>12</td>
<td>0</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>Security Assessment</td>
<td>3</td>
<td>8</td>
<td>0</td>
<td>3</td>
<td>2</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>Situational Awareness</td>
<td>1</td>
<td>3</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>System and Communications Protection</td>
<td>2</td>
<td>27</td>
<td>2</td>
<td>2</td>
<td>15</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>System and Information Integrity</td>
<td>4</td>
<td>13</td>
<td>4</td>
<td>3</td>
<td>3</td>
<td>1</td>
<td>2</td>
</tr>
</tbody>
</table>

### Total Practices per Level

<table>
<thead>
<tr>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
<th>Level 4</th>
<th>Level 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>17</td>
<td>55</td>
<td>58</td>
<td>26</td>
<td>15</td>
</tr>
</tbody>
</table>
REQUIREMENTS FOR CONTRACTORS

Compliance is not a one-time activity – It requires building an enterprise information security program that continuously assesses and manages risks, protects covered information and systems used for processing, storage and transmission, and monitors and detects threats with the ability to report incidents.

Organization Size is not a consideration – All companies must comply. It only takes one user, one system to cause a cyber breach.

Not just IT – The requirements covers your People, Policies, Processes, Technologies, Physical and Environmental, Supply Chain, etc..

You can’t outsource your compliance responsibility. You have to be able to document how your service providers/cloud services meet the control requirements.
CMMC Compliance Timeline

ASSESSMENT ECOSYSTEM TIMELINE

1. Formation
   - January 2020

2. Ecosystem Design & Build
   - February 2020

3. C3PAO & Role Applications
   - Summer 2020

4. Provisional Program... Testing the Design
   - Summer/Fall 2020

5. Training Criteria Publication
   - Fall 2020

6. Certified Training
   - Winter 2020/21

7. Ecosystem Go-Live
   - Winter/Spring 2021

ORGANIZATIONS SEEKING CERTIFICATION

1. Learn and Understand about CMMC Requirements
2. Identify Gaps
3. Remediates Gaps and Get Ready
4. Bid on Contracts
   - Conduct Assessment
   - Earn Certification

MCGLOBALTECH
AGILE ○ INNOVATIVE ○ GLOBAL
CONSEQUENCES FOR CONTRACTORS

Companies unable to demonstrate CMMC and NIST 800-171 compliance will be severely impacted as Contracting Officers and Prime Contractors will require DFARS compliance and CMMC certification as a pre-requisite to [continue] doing business with the DOD.

For companies currently doing business with the DOD, consequences of non-compliance may include contract termination for default or convenience, suspension or debarment, breach of contract damages, liquidated damages, and False Claims Act damages.
Our Managed Compliance Service (MCS) provides **full life-cycle security compliance support** to help fellow small businesses meet regulatory and business security goals.

Regardless of company size or service offering, the MCS helps you build and mature an enterprise information security program that protects your mission-critical People, Processes and Technologies necessary to protect you and your customers from growing cyber threats and increasingly complex regulatory requirements.
Full Life-Cycle Security

Security Requirements Definition
- NIST 800 Series Requirements
- DOD 8500 Series Requirements
- FIPS Pub 200
- ISO 27001
- PCI DSS
- HIPAA
- COBIT
- SOX

Security Design and Engineering
- Security Architecture Design & Implementation
  - Security Risk Assessment
  - Security Control Development & Implementation

Security Test, Validation and Reporting
- Code Review
- Fuzz Testing
- Security Audit
- Vulnerability Testing
- Penetration Testing
- Security Control Assessment

Security Documentation and Response
- NIST 800 Series
- DOD 8500 Series
- Forensic Analysis
- Incident Response
- Continuous Monitoring
- Plan of Action & Milestones
MCGlobalTech MCS Goals

Security and Compliance Goals

- Maintain compliance documentation
- Build security policy framework
- Perform vulnerability management
- Perform security controls testing
- Track and manage security risks
- Educate and train users and system administrators
- Provide security monitoring throughout environment
The MCS provides a CMMC/NIST 800-171 baseline compliance audit against all required controls based on appropriate level and generates the required compliance documentation i.e. System Security Plan (SSP) which documents state of compliance and Plan of Action and Milestones (POAM) which documents identified gaps and remediation plans and timelines.

POAM remediation is then tracked, validated and documented with quarterly assessments thus improving compliance posture and mature security program. Required on-going security controls assessments, vulnerability and risk assessments continuous monitoring, and penetration tests are scheduled as appropriate intervals.
The MCGlobalTech Managed Compliance Service provides an efficient and cost-effective pathway to the development of the compliance program and becoming CMMC-ready as quickly as possible. Our compliance analysts and security engineers partner with you every step of the way from determining appropriate scope and compliance levels to documenting policies, plans, and milestone.
Managing a NIST 800-171/ CMMC Level 3 compliance program requires implementation, documentation, and monitoring of 130 controls to protect CUI and FCI. The MCS provides clients a compliance management dashboard to track required control implementation status and activities.
## Managed Compliance Schedule

<table>
<thead>
<tr>
<th>Quarter 1</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>❑ Documentation Review (Policies, Network Diagrams, Assets, etc.)</td>
<td></td>
</tr>
<tr>
<td>❑ Compliance Scoping and CMMC Level Determination</td>
<td></td>
</tr>
<tr>
<td>❑ CMMC / NIST 800-171 Policies and Procedures Development</td>
<td></td>
</tr>
<tr>
<td>❑ Controls Audit and Validation</td>
<td></td>
</tr>
<tr>
<td>❑ System Security Plan (SSP) Development</td>
<td></td>
</tr>
<tr>
<td>❑ Plan of Action &amp; Milestone (POAM) Development</td>
<td></td>
</tr>
<tr>
<td>❑ *Discounted Security Support Services</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Quarter 2</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>❑ Plan of Action &amp; Milestone (POAM) Review/Update</td>
<td></td>
</tr>
<tr>
<td>❑ System Security Plan (SSP) Review/Update</td>
<td></td>
</tr>
<tr>
<td>❑ *Discounted Security Support Services</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Quarter 3</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>❑ Plan of Action &amp; Milestone (POAM) Review/Update</td>
<td></td>
</tr>
<tr>
<td>❑ System Security Plan (SSP) Review/Update</td>
<td></td>
</tr>
<tr>
<td>❑ *Discounted Security Support Services</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Quarter 4</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>❑ Plan of Action &amp; Milestone (POAM) Review/Update</td>
<td></td>
</tr>
<tr>
<td>❑ System Security Plan (SSP) Review/Update</td>
<td></td>
</tr>
<tr>
<td>❑ *Discounted Security Support Services</td>
<td></td>
</tr>
</tbody>
</table>
Managed Security Service

The MCGlobalTech Managed Security Service (MSS) provides 24/7 monitoring of all end user systems (laptops, desktops, mobile devices, servers) and Internet-facing devices (routers, firewalls, webservers) for near real-time detect and response to cyber threats and vulnerabilities.

Our MSS also helps small business clients meet security audit, monitoring and incident reporting compliance requirements of the DFARS 7012/NIST 800-171.
MCGlobalTech’s Principals have worked for and with large and small contracting and consulting firms. We have provided security expertise throughout the federal government including the Department of Defense, Intelligence and Federal Civilian Agencies. We have also provided security services to financial, healthcare and various commercial sector organizations throughout the country.

A list of some of our clients we’ve helped meet the CMMC NIST 800-171 compliance requirements is provided in the following table.
Key Takeaways

➢ Size doesn’t matter.

➢ IT service providers can help but can’t do it all.

➢ Compliance is no longer optional.

➢ We can help.
About MCGlobalTech

- Mission Critical Global Technology Group (MCGlobalTech) is a minority owned, small business founded by industry leaders to provide strategic advisory and security consulting services to public and private sector business managers to better align technology and security programs with organizational mission and business goals.

- The Principals at MCGlobalTech have been providing Information Security services to the Federal Government and the private sector for over 25 years.
Leadership

- **William J McBorrough**, MSIA, CISSP, CISA, CRISC
- Chief Security Advisor, **MCGlobalTech**
- 20+ years Information Security Professional
- 12 years Adjunct College Professor - Cybersecurity
- Cybersecurity Governance Risk Compliance Expert
- NIST 800-171/CMMC Subject Matter Expert
At MCGlobalTech, we believe that strong values create long term relationships with our customers, employees, partners and the communities we serve. At the heart of everything we do, our corporate values are:

- Providing customer satisfaction
- Delivering innovative solutions
- Empowering staff for success
- Promoting Entrepreneurial spirit
- Maintaining technical excellence
MCGlobalTech provides innovative, cost-effective, mission-critical solutions to manage security governance, risk and compliance.

We specialize in the following service offerings:

- Security Program Development
- Managed vCISO Services
- Security Risk Management
- CMMC/NIST Compliance
- Continuous Monitoring
- Technical Security Assessments
Mission Critical Global Technology Group
1325 G Street, NW
Suite 500
Washington, District of Columbia 20005
Phone: 202.355.9448
Email: Info@mcglobaltech.com

William J. McMorrough
CEO/Chief Security Advisor
wjm4@mcglobaltech.com
(202) 355-9448 x101
(571) 249-4677 (cell)

Sales Division
Corporate Headquarters
sales@mcglobaltech.com
(202) 355-9448 x200