Protect your organization from going out of business?
A Cyber Security Management System Implementation
NIST/MEP

400 CENTERS NATIONWIDE

http://www.mep.nist.gov

18,200 jobs created & retained

$652 million in cost savings

$2.25 billion in new & retained sales
TMAC works with businesses to accelerate their **profitable** growth and **competitiveness** by developing and improving their products, processes, technologies & people.
Overview

- Why Worry?
- Focus on cyber security now?
- Security Management System
- Can you protect yourself?
- Wrap-up
WHAT'S THERE TO WORRY ABOUT?
Global security incidents (GSiSS 2015)

48%

Global smartphone users (eMarketer)

22%

Global GDP (OECD)

21%

Security incidents outpace GDP and mobile phone growth

The percentage of growth for global security incidents is more than double global GDP and global smartphone users combined.

# Top Business Risks 2019

## Top 5 risks for small enterprise companies (<€250mn annual revenues)

<table>
<thead>
<tr>
<th>Rank</th>
<th>Risk Description</th>
<th>Percent</th>
<th>2018 rank</th>
<th>Trend</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Cyber incidents (e.g. cyber crime, IT failure/outage, data breaches, fines and penalties)</td>
<td>32%</td>
<td>2 (30%)</td>
<td>▲</td>
</tr>
<tr>
<td></td>
<td>Changes in legislation and regulation (e.g. trade wars and tariffs, sanctions)</td>
<td>29%</td>
<td>5 (22%)</td>
<td>▲</td>
</tr>
</tbody>
</table>

## Top 5 risks for mid-size companies (€250mn to €500mn annual revenues)

<table>
<thead>
<tr>
<th>Rank</th>
<th>Risk Description</th>
<th>Percent</th>
<th>2018 rank</th>
<th>Trend</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Business interruption (incl. supply chain disruption)</td>
<td>38%</td>
<td>2 (37%)</td>
<td>▲</td>
</tr>
<tr>
<td>2</td>
<td>Cyber incidents (e.g. cyber crime, IT failure/outage, data breaches, fines and penalties)</td>
<td>32%</td>
<td>1 (39%)</td>
<td>▼</td>
</tr>
<tr>
<td>3</td>
<td>Natural catastrophes (e.g. storm, flood, earthquake)</td>
<td>29%</td>
<td>3 (32%)</td>
<td>=</td>
</tr>
<tr>
<td>4</td>
<td>Changes in legislation and regulation (e.g. trade wars and tariffs, sanctions, protectionism, Brexit, Euro-zone disintegration)</td>
<td>24%</td>
<td>6 (18%)</td>
<td>▲</td>
</tr>
<tr>
<td>5</td>
<td>Market developments (e.g. volatility, intensified competition/new entrants, M&amp;A, market stagnation, market fluctuation)</td>
<td>23%</td>
<td>5 (21%)</td>
<td>=</td>
</tr>
</tbody>
</table>

Source: Allianz Global Corporate & Specialty. Figures represent how often a risk was selected as a percentage of all responses for that company size. Responses = 617. Figures don’t add up to 100% as up to three risks could be selected.
Reported Cyber Incidents by Sector

US Reported Cyber Incidents by Critical Infrastructure Sector.
(Source: Department of Homeland Security 2015.)
Average Financial Loss Per Cyber-Attack

Small Biz
$0.41M
(Revenue <$100M)

Medium Biz
$1.3M
(Revenue $100M-$1B)

Large Biz
$5.9M
(Revenue >$1B)
Images of some travelers stolen in data breach, Customs and Border Protection says

Mumbai-based firm loses Rs 130 crore to hackers in con job

The hackers sent emails to the head of the Indian subsidiary of the firm through an email account, which looked similar to that of the group CEO, a police official said.

British Airways faces record £183m fine for data breach

Baltimore hit by ransomware attack, forcing officials to shut down city’s servers

Cyber criminals are using stolen doctor credentials on the dark web to enrich themselves

Average Healthcare Cyberattack Recovery Cost: $1.4 Million

Florida City Fires IT Employee After Paying $460,000 Bitcoin Ransom to Hackers

Airbus hit by series of cyber attacks on suppliers
AUSTIN, Tex. (KBTX) - The Texas Department of Transportation's website and web services are down after a ransomware attack.

The full released statement is below from the official TxDOT Twitter account:

"The Texas Department of Transportation determined that on May 14, 2020, there was unauthorized access to the agency's network in a ransomware event. TxDOT immediately took steps to isolate the incident and shut down further unauthorized access. In addition, the agency promptly began working with federal law enforcement."
Why the focus on Cyber Security now?
The 4th Revolution in Manufacturing Technology

1800
Industry 1.0
The Industrial Revolution begins. Mechanization of manufacturing with the introduction of steam and water power

1900
Industry 2.0
Mass production assembly lines using electrical power

2000
Industry 3.0
Automated production using electronics, programmable logic controllers (PLC), IT systems and robotics

The 'Smart Factory'. Autonomous decision making of cyber physical systems using machine learning and Big Data analysis. Interoperability through IoT and cloud technology.
Smart Factory Design Principles

- Interoperability
- Information Transparency
- Technical Assistance
- Decentralized Decisions
In essence, a lot of data moving around, yet not a lot of emphasis in data security
Which Would YOU Target?

- Motion and impact sensors
- Video cameras
- 24/7/365 professionals
National Institute of Standards and Technology (NIST)
Which IT security guidelines or standards does your company comply with?

Data Source:
2018 State of Cybersecurity in Small & Medium Size Businesses
Cyber Security Standards

- NIST SP 800-171
- Cybersecurity Maturity Model Certification (CMMC)
- ISO 27001:2013 – Can be certified.
First published in 2005, the latest revision in 2013
Risk management as the central idea
Provides requirements to establish an Information Security Management System
Establishes safeguards (or controls) to be implemented in the form of policies, procedures and technical implementation
Can get certified via a certifying body.
DFARS

- Stands for Defense Federal Acquisition Regulation Supplement
- Applies all DOD contractors & subcontractors
- Sets up guidelines to safeguard defense information
- Requires reporting of cyber incidents
- Refers to NIST 800–171 for implementation

Need more information: https://www.nist.gov/mep/cybersecurity-resources-manufacturers/dfars-compliance
NIST’s Computer Security Publications

- Non-regulatory agency of the U.S. Department of Commerce
- **NIST does not regulate, audit or certify compliance.**
- NIST provides neutral guidance, technical expertise, and reference materials for use by government agencies and industry organizations.
- NIST generated the document SP 800-171 originally in 2015.
- It was updated with Revision 2 in February 2020.
DOD, GSA and NASA Suppliers

- Compliance with NIST SP 800-171 became a requirement as of December 31, 2017 with DFARS 252.204-7012 and FAR 52.204-21.

- DOD is assessing contractor compliance during the contract award process based on self reporting.

- There is currently **NO Accredited 3rd Party Audit Program.**
- Stands for Cyber Security Maturity Model Certification
- Process initiated in March 2019
- A collaborative effort between OUSD (AS), DOD stakeholders, UARC’s and other federal research centers
- Adds a verification component to existing regulation (DFARS 252.204–7012)
- The intent is for certified independent 3rd party organizations to conduct audits and inform risk.
- Certifications to 5 CMMC Levels; some designed for Small Businesses
## CMMC vs. ISO 27001:2013

<table>
<thead>
<tr>
<th>ISO IEC 27001</th>
<th>CMMC</th>
</tr>
</thead>
<tbody>
<tr>
<td>A.9.1.2 Users shall only be provided with access to the network and network services that they have been specifically authorized to use.</td>
<td>AC.2.008- Use non-privileged accounts or roles when accessing non-security functions.</td>
</tr>
<tr>
<td>A.9.4.2 Where required by the access control policy, access to systems and applications shall be controlled by a secure log on procedure.</td>
<td>AC.2.009- Limit unsuccessful logon attempts.</td>
</tr>
<tr>
<td>A.9.3.1 Users shall be required to follow the organization’s practices in the use of secret authentication information.</td>
<td>IA.3.083-Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.</td>
</tr>
<tr>
<td></td>
<td>IA3.084-Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.</td>
</tr>
</tbody>
</table>
NIST Cybersecurity Framework

- Designed to reduce risk by improving the management of cybersecurity risk
- Helps create plans to determine what to do before, during and after a cyber incident
Implementing SP 800-171

- Security requirements are organized into 14 families

- Implemented through
  - technical methods
  - security policies
  - procedures
  - best practices

<table>
<thead>
<tr>
<th>NIST SP 800-171 “Families”</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control - AC</td>
</tr>
<tr>
<td>Awareness and Training - AT</td>
</tr>
<tr>
<td>Audit and Accountability - AU</td>
</tr>
<tr>
<td>Configuration Management - CM</td>
</tr>
<tr>
<td>Identification and Authentication - IA</td>
</tr>
<tr>
<td>Incident Response - IR</td>
</tr>
<tr>
<td>Maintenance - MA</td>
</tr>
<tr>
<td>Media Protection - MP</td>
</tr>
<tr>
<td>Personnel Security - PS</td>
</tr>
<tr>
<td>Physical Protection - PE</td>
</tr>
<tr>
<td>Systems and Communications Protection - SC</td>
</tr>
<tr>
<td>Security Assessment - CA</td>
</tr>
<tr>
<td>Risk Assessment - RM</td>
</tr>
<tr>
<td>System and Information Integrity - SI</td>
</tr>
</tbody>
</table>
# Implementing SP 800-171

## NIST 800-171 rev2 Summary

<table>
<thead>
<tr>
<th>AC</th>
<th>AT</th>
<th>AU</th>
<th>CM</th>
<th>IA</th>
<th>IR</th>
<th>MT</th>
<th>MP</th>
<th>PS</th>
<th>PE</th>
<th>RA</th>
<th>CA</th>
<th>SC</th>
<th>SI</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.1</td>
<td>3.2.1</td>
<td>3.3.1</td>
<td>3.4.1</td>
<td>3.5.1</td>
<td>3.6.1</td>
<td>3.7.1</td>
<td>3.8.1</td>
<td>3.9.1</td>
<td>3.10.1</td>
<td>3.11.1</td>
<td>3.12.1</td>
<td>3.13.1</td>
<td>3.14.1</td>
</tr>
<tr>
<td>3.1.2</td>
<td>3.2.2</td>
<td>3.3.2</td>
<td>3.4.2</td>
<td>3.5.2</td>
<td>3.6.2</td>
<td>3.7.2</td>
<td>3.8.2</td>
<td>3.9.2</td>
<td>3.10.2</td>
<td>3.11.2</td>
<td>3.12.2</td>
<td>3.13.2</td>
<td>3.14.2</td>
</tr>
<tr>
<td>3.1.3</td>
<td>3.2.3</td>
<td>3.3.3</td>
<td>3.4.3</td>
<td>3.5.3</td>
<td>3.6.3</td>
<td>3.7.3</td>
<td>3.8.3</td>
<td>3.9.3</td>
<td>3.10.3</td>
<td>3.11.3</td>
<td>3.12.3</td>
<td>3.13.3</td>
<td>3.14.3</td>
</tr>
<tr>
<td>3.1.4</td>
<td>3.2.4</td>
<td>3.3.4</td>
<td>3.4.4</td>
<td>3.5.4</td>
<td>3.6.4</td>
<td>3.7.4</td>
<td>3.8.4</td>
<td>3.9.4</td>
<td>3.10.4</td>
<td>3.11.4</td>
<td>3.12.4</td>
<td>3.13.4</td>
<td>3.14.4</td>
</tr>
<tr>
<td>3.1.5</td>
<td>3.2.5</td>
<td>3.3.5</td>
<td>3.4.5</td>
<td>3.5.5</td>
<td>3.6.5</td>
<td>3.7.5</td>
<td>3.8.5</td>
<td>3.9.5</td>
<td>3.10.5</td>
<td>3.11.5</td>
<td>3.12.5</td>
<td>3.13.5</td>
<td>3.14.5</td>
</tr>
<tr>
<td>3.1.6</td>
<td>3.2.6</td>
<td>3.3.6</td>
<td>3.4.6</td>
<td>3.5.6</td>
<td>3.6.6</td>
<td>3.7.6</td>
<td>3.8.6</td>
<td>3.9.6</td>
<td>3.10.6</td>
<td>3.11.6</td>
<td>3.12.6</td>
<td>3.13.6</td>
<td>3.14.6</td>
</tr>
<tr>
<td>3.1.7</td>
<td>3.2.7</td>
<td>3.3.7</td>
<td>3.4.7</td>
<td>3.5.7</td>
<td>3.6.7</td>
<td>3.7.7</td>
<td>3.8.7</td>
<td>3.9.7</td>
<td>3.10.7</td>
<td>3.11.7</td>
<td>3.12.7</td>
<td>3.13.7</td>
<td>3.14.7</td>
</tr>
<tr>
<td>3.1.8</td>
<td>3.2.8</td>
<td>3.3.8</td>
<td>3.4.8</td>
<td>3.5.8</td>
<td>3.6.8</td>
<td>3.7.8</td>
<td>3.8.8</td>
<td>3.9.8</td>
<td>3.10.8</td>
<td>3.11.8</td>
<td>3.12.8</td>
<td>3.13.8</td>
<td>3.14.8</td>
</tr>
<tr>
<td>3.1.9</td>
<td>3.2.9</td>
<td>3.3.9</td>
<td>3.4.9</td>
<td>3.5.9</td>
<td>3.6.9</td>
<td>3.7.9</td>
<td>3.8.9</td>
<td>3.9.9</td>
<td>3.10.9</td>
<td>3.11.9</td>
<td>3.12.9</td>
<td>3.13.9</td>
<td>3.14.9</td>
</tr>
<tr>
<td>3.1.10</td>
<td>3.2.10</td>
<td>3.3.10</td>
<td>3.4.10</td>
<td>3.5.10</td>
<td>3.6.10</td>
<td>3.7.10</td>
<td>3.8.10</td>
<td>3.9.10</td>
<td>3.10.10</td>
<td>3.11.10</td>
<td>3.12.10</td>
<td>3.13.10</td>
<td>3.14.10</td>
</tr>
<tr>
<td>3.1.11</td>
<td>3.2.11</td>
<td>3.3.11</td>
<td>3.4.11</td>
<td>3.5.11</td>
<td>3.6.11</td>
<td>3.7.11</td>
<td>3.8.11</td>
<td>3.9.11</td>
<td>3.10.11</td>
<td>3.11.11</td>
<td>3.12.11</td>
<td>3.13.11</td>
<td>3.14.11</td>
</tr>
<tr>
<td>3.1.15</td>
<td>3.2.15</td>
<td>3.3.15</td>
<td>3.4.15</td>
<td>3.5.15</td>
<td>3.6.15</td>
<td>3.7.15</td>
<td>3.8.15</td>
<td>3.9.15</td>
<td>3.10.15</td>
<td>3.11.15</td>
<td>3.12.15</td>
<td>3.13.15</td>
<td>3.14.15</td>
</tr>
<tr>
<td>3.1.16</td>
<td>3.2.16</td>
<td>3.3.16</td>
<td>3.4.16</td>
<td>3.5.16</td>
<td>3.6.16</td>
<td>3.7.16</td>
<td>3.8.16</td>
<td>3.9.16</td>
<td>3.10.16</td>
<td>3.11.16</td>
<td>3.12.16</td>
<td>3.13.16</td>
<td>3.14.16</td>
</tr>
</tbody>
</table>

- **AC**: Administrative (e.g., policies, standards & procedures)
- **AT**: Assigned Tasks To Cybersecurity Personnel
- **AU**: Assigned Tasks To IT Personnel
- **CM**: Assigned Tasks To Application/Asset/Process Owner
- **IA**: Configuration or Software Solution
- **IR**: Hardware Solution
- **MT**: Software or Hardware Solution
- **MP**: Technical Configurations (e.g., security settings)
CMMC Model

In addition to the 14 “Families” found in SP 800-171, there are 3 additional “Domains” included in CMMC.

<table>
<thead>
<tr>
<th>NIST SP 800-171 “Families” + CMMC “Domains”</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control - AC</td>
</tr>
<tr>
<td>Awareness and Training - AT</td>
</tr>
<tr>
<td>Audit and Accountability - AU</td>
</tr>
<tr>
<td>Configuration Management - CM</td>
</tr>
<tr>
<td>Identification and Authentication - IA</td>
</tr>
<tr>
<td>Incident Response - IR</td>
</tr>
<tr>
<td>Maintenance - MA</td>
</tr>
<tr>
<td>Asset Management - AM</td>
</tr>
<tr>
<td>Recovery - RE</td>
</tr>
<tr>
<td>Media Protection - MP</td>
</tr>
<tr>
<td>Personnel Security - PS</td>
</tr>
<tr>
<td>Physical Protection - PE</td>
</tr>
<tr>
<td>Systems and Communications Protection - SC</td>
</tr>
<tr>
<td>Security Assessment - CA</td>
</tr>
<tr>
<td>Risk Assessment - RM</td>
</tr>
<tr>
<td>System and Information Integrity - SI</td>
</tr>
<tr>
<td>Situational Awareness - SA</td>
</tr>
</tbody>
</table>
CMMC Levels

Maturity Level Certification will require implementation of ALL practices required for that level.

➢ There can be no PoAM’s for outstanding requirements.
CMMC vs. ISO 27001:2013

<table>
<thead>
<tr>
<th>CMMC</th>
<th>ISO 27001:2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>17 Domains</td>
<td>14 Domains</td>
</tr>
<tr>
<td>43 Objectives</td>
<td>35 Objectives</td>
</tr>
<tr>
<td>130 Practices (@ level 3)</td>
<td>113 Controls</td>
</tr>
<tr>
<td>Specific and technical requirements</td>
<td>High level (generic) requirements</td>
</tr>
</tbody>
</table>

- Customers that require NIST 800-171 compliance MAY be willing to accept ISO 27001:2013 certification.
- Customers who require compliance with a specific CMMC level are not expected to accept ISO 27001:2013 Certification.
<table>
<thead>
<tr>
<th>Level 1</th>
<th>Description of Practices</th>
<th>Description of Processes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Basic cybersecurity</td>
<td>Practices are performed, at least in an ad hoc manner</td>
</tr>
<tr>
<td></td>
<td>Achievable for small companies</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Subset of universally accepted common practices</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Limited resistance against data exfiltration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Limited resilience against malicious actions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Inclusive of universally accepted cyber security best practices</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Resilient against unskilled threat actors</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Minor resistance against data exfiltration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Minor resilience against malicious actions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Coverage of all NIST SP 800-171 rev 1 controls</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Additional practices beyond the scope of all protection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Resilient against moderately skilled threat actors</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Moderate resistance against data exfiltration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Moderate resilience against malicious actions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Comprehensive knowledge of cyber assets</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Advanced and customized cybersecurity practices</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Resilient against advanced threat actors</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Defensive responses approach machine speed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Increased resistance and detection of data exfiltration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Complete and continuous knowledge of cyber assets</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Highly advanced cybersecurity practices</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Reserved for the most critical systems</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Resilient against the most-advanced threat actors</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Defensive responses performed at machine speed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Machine performed analytics and defensive actions</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Resistant against, and detection of, data exfiltration</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Autonomous knowledge of cyber assets</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Continuous improvement across the enterprise</td>
<td></td>
</tr>
</tbody>
</table>
Implementing SP 800-171

Everything CMMC is DRAFT
# Implementing SP 800-171

CMMC Level 1
CMMC Level 2

## Everything CMMC is DRAFT

### NSP-800-171 rev2 Summary

<table>
<thead>
<tr>
<th>AC</th>
<th>AT</th>
<th>AU</th>
<th>CM</th>
<th>IA</th>
<th>IR</th>
<th>MT</th>
<th>MP</th>
<th>PS</th>
<th>PE</th>
<th>RA</th>
<th>CA</th>
<th>SC</th>
<th>SI</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.1</td>
<td>3.2.1</td>
<td>3.3.1</td>
<td>3.4.1</td>
<td>3.5.1</td>
<td>3.6.1</td>
<td>3.7.1</td>
<td>3.8.1</td>
<td>3.9.1</td>
<td>3.10.1</td>
<td>3.11.1</td>
<td>3.12.1</td>
<td>3.13.1</td>
<td>3.14.1</td>
</tr>
<tr>
<td>3.1.2</td>
<td>3.2.2</td>
<td>3.3.2</td>
<td>3.4.2</td>
<td>3.5.2</td>
<td>3.6.2</td>
<td>3.7.2</td>
<td>3.8.2</td>
<td>3.9.2</td>
<td>3.10.2</td>
<td>3.11.2</td>
<td>3.12.2</td>
<td>3.13.2</td>
<td>3.14.2</td>
</tr>
<tr>
<td>3.1.3</td>
<td>3.2.3</td>
<td>3.3.3</td>
<td>3.4.3</td>
<td>3.5.3</td>
<td>3.6.3</td>
<td>3.7.3</td>
<td>3.8.3</td>
<td>3.9.3</td>
<td>3.10.3</td>
<td>3.11.3</td>
<td>3.12.3</td>
<td>3.13.3</td>
<td>3.14.3</td>
</tr>
<tr>
<td>3.1.4</td>
<td>3.2.4</td>
<td>3.3.4</td>
<td>3.4.4</td>
<td>3.5.4</td>
<td>3.6.4</td>
<td>3.7.4</td>
<td>3.8.4</td>
<td>3.9.4</td>
<td>3.10.4</td>
<td>3.11.4</td>
<td>3.12.4</td>
<td>3.13.4</td>
<td>3.14.4</td>
</tr>
<tr>
<td>3.1.5</td>
<td>3.2.5</td>
<td>3.3.5</td>
<td>3.4.5</td>
<td>3.5.5</td>
<td>3.6.5</td>
<td>3.7.5</td>
<td>3.8.5</td>
<td>3.9.5</td>
<td>3.10.5</td>
<td>3.11.5</td>
<td>3.12.5</td>
<td>3.13.5</td>
<td>3.14.5</td>
</tr>
<tr>
<td>3.1.6</td>
<td>3.2.6</td>
<td>3.3.6</td>
<td>3.4.6</td>
<td>3.5.6</td>
<td>3.6.6</td>
<td>3.7.6</td>
<td>3.8.6</td>
<td>3.9.6</td>
<td>3.10.6</td>
<td>3.11.6</td>
<td>3.12.6</td>
<td>3.13.6</td>
<td>3.14.6</td>
</tr>
<tr>
<td>3.1.7</td>
<td>3.2.7</td>
<td>3.3.7</td>
<td>3.4.7</td>
<td>3.5.7</td>
<td>3.6.7</td>
<td>3.7.7</td>
<td>3.8.7</td>
<td>3.9.7</td>
<td>3.10.7</td>
<td>3.11.7</td>
<td>3.12.7</td>
<td>3.13.7</td>
<td>3.14.7</td>
</tr>
<tr>
<td>3.1.8</td>
<td>3.2.8</td>
<td>3.3.8</td>
<td>3.4.8</td>
<td>3.5.8</td>
<td>3.6.8</td>
<td>3.7.8</td>
<td>3.8.8</td>
<td>3.9.8</td>
<td>3.10.8</td>
<td>3.11.8</td>
<td>3.12.8</td>
<td>3.13.8</td>
<td>3.14.8</td>
</tr>
<tr>
<td>3.1.9</td>
<td>3.2.9</td>
<td>3.3.9</td>
<td>3.4.9</td>
<td>3.5.9</td>
<td>3.6.9</td>
<td>3.7.9</td>
<td>3.8.9</td>
<td>3.9.9</td>
<td>3.10.9</td>
<td>3.11.9</td>
<td>3.12.9</td>
<td>3.13.9</td>
<td>3.14.9</td>
</tr>
<tr>
<td>3.1.10</td>
<td>3.2.10</td>
<td>3.3.10</td>
<td>3.4.10</td>
<td>3.5.10</td>
<td>3.6.10</td>
<td>3.7.10</td>
<td>3.8.10</td>
<td>3.9.10</td>
<td>3.10.10</td>
<td>3.11.10</td>
<td>3.12.10</td>
<td>3.13.10</td>
<td>3.14.10</td>
</tr>
<tr>
<td>3.1.11</td>
<td>3.2.11</td>
<td>3.3.11</td>
<td>3.4.11</td>
<td>3.5.11</td>
<td>3.6.11</td>
<td>3.7.11</td>
<td>3.8.11</td>
<td>3.9.11</td>
<td>3.10.11</td>
<td>3.11.11</td>
<td>3.12.11</td>
<td>3.13.11</td>
<td>3.14.11</td>
</tr>
<tr>
<td>3.1.15</td>
<td>3.2.15</td>
<td>3.3.15</td>
<td>3.4.15</td>
<td>3.5.15</td>
<td>3.6.15</td>
<td>3.7.15</td>
<td>3.8.15</td>
<td>3.9.15</td>
<td>3.10.15</td>
<td>3.11.15</td>
<td>3.12.15</td>
<td>3.13.15</td>
<td>3.14.15</td>
</tr>
<tr>
<td>3.1.16</td>
<td>3.2.16</td>
<td>3.3.16</td>
<td>3.4.16</td>
<td>3.5.16</td>
<td>3.6.16</td>
<td>3.7.16</td>
<td>3.8.16</td>
<td>3.9.16</td>
<td>3.10.16</td>
<td>3.11.16</td>
<td>3.12.16</td>
<td>3.13.16</td>
<td>3.14.16</td>
</tr>
</tbody>
</table>

Legend:
- **Administrative (e.g., policies, standards & procedures)**
- **Assigned Tasks To Cybersecurity Personnel**
- **Assigned Tasks To IT Personnel**
- **Assigned Tasks To Application/Asset/Process Owner**
- **Configuration or Software Solution**
- **Hardware Solution**
- **Software or Hardware Solution**
Implementing SP 800-171

Everything CMMC is DRAFT

NTSP-800-171 rev2 Summary

<table>
<thead>
<tr>
<th>AC</th>
<th>AT</th>
<th>AU</th>
<th>CM</th>
<th>IA</th>
<th>IR</th>
<th>MT</th>
<th>MP</th>
<th>PS</th>
<th>PE</th>
<th>RA</th>
<th>CA</th>
<th>SC</th>
<th>SI</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.1.1</td>
<td>3.2.1</td>
<td>3.3.1</td>
<td>3.4.1</td>
<td>3.5.1</td>
<td>3.6.1</td>
<td>3.7.1</td>
<td>3.8.1</td>
<td>3.9.1</td>
<td>3.10.1</td>
<td>3.11.1</td>
<td>3.12.1</td>
<td>3.13.1</td>
<td>3.14.1</td>
</tr>
<tr>
<td>3.1.2</td>
<td>3.2.2</td>
<td>3.3.2</td>
<td>3.4.2</td>
<td>3.5.2</td>
<td>3.6.2</td>
<td>3.7.2</td>
<td>3.8.2</td>
<td>3.9.2</td>
<td>3.10.2</td>
<td>3.11.2</td>
<td>3.12.2</td>
<td>3.13.2</td>
<td>3.14.2</td>
</tr>
<tr>
<td>3.1.3</td>
<td>3.2.3</td>
<td>3.3.3</td>
<td>3.4.3</td>
<td>3.5.3</td>
<td>3.6.3</td>
<td>3.7.3</td>
<td>3.8.3</td>
<td>3.9.3</td>
<td>3.10.3</td>
<td>3.11.3</td>
<td>3.12.3</td>
<td>3.13.3</td>
<td>3.14.3</td>
</tr>
<tr>
<td>3.1.4</td>
<td>3.2.4</td>
<td>3.3.4</td>
<td>3.4.4</td>
<td>3.5.4</td>
<td>3.6.4</td>
<td>3.7.4</td>
<td>3.8.4</td>
<td>3.9.4</td>
<td>3.10.4</td>
<td>3.11.4</td>
<td>3.12.4</td>
<td>3.13.4</td>
<td>3.14.4</td>
</tr>
<tr>
<td>3.1.5</td>
<td>3.2.5</td>
<td>3.3.5</td>
<td>3.4.5</td>
<td>3.5.5</td>
<td>3.6.5</td>
<td>3.7.5</td>
<td>3.8.5</td>
<td>3.9.5</td>
<td>3.10.5</td>
<td>3.11.5</td>
<td>3.12.5</td>
<td>3.13.5</td>
<td>3.14.5</td>
</tr>
<tr>
<td>3.1.6</td>
<td>3.2.6</td>
<td>3.3.6</td>
<td>3.4.6</td>
<td>3.5.6</td>
<td>3.6.6</td>
<td>3.7.6</td>
<td>3.8.6</td>
<td>3.9.6</td>
<td>3.10.6</td>
<td>3.11.6</td>
<td>3.12.6</td>
<td>3.13.6</td>
<td>3.14.6</td>
</tr>
<tr>
<td>3.1.7</td>
<td>3.2.7</td>
<td>3.3.7</td>
<td>3.4.7</td>
<td>3.5.7</td>
<td>3.6.7</td>
<td>3.7.7</td>
<td>3.8.7</td>
<td>3.9.7</td>
<td>3.10.7</td>
<td>3.11.7</td>
<td>3.12.7</td>
<td>3.13.7</td>
<td>3.14.7</td>
</tr>
<tr>
<td>3.1.8</td>
<td>3.2.8</td>
<td>3.3.8</td>
<td>3.4.8</td>
<td>3.5.8</td>
<td>3.6.8</td>
<td>3.7.8</td>
<td>3.8.8</td>
<td>3.9.8</td>
<td>3.10.8</td>
<td>3.11.8</td>
<td>3.12.8</td>
<td>3.13.8</td>
<td>3.14.8</td>
</tr>
<tr>
<td>3.1.9</td>
<td>3.2.9</td>
<td>3.3.9</td>
<td>3.4.9</td>
<td>3.5.9</td>
<td>3.6.9</td>
<td>3.7.9</td>
<td>3.8.9</td>
<td>3.9.9</td>
<td>3.10.9</td>
<td>3.11.9</td>
<td>3.12.9</td>
<td>3.13.9</td>
<td>3.14.9</td>
</tr>
<tr>
<td>3.1.10</td>
<td>3.2.10</td>
<td>3.3.10</td>
<td>3.4.10</td>
<td>3.5.10</td>
<td>3.6.10</td>
<td>3.7.10</td>
<td>3.8.10</td>
<td>3.9.10</td>
<td>3.10.10</td>
<td>3.11.10</td>
<td>3.12.10</td>
<td>3.13.10</td>
<td>3.14.10</td>
</tr>
<tr>
<td>3.1.11</td>
<td>3.2.11</td>
<td>3.3.11</td>
<td>3.4.11</td>
<td>3.5.11</td>
<td>3.6.11</td>
<td>3.7.11</td>
<td>3.8.11</td>
<td>3.9.11</td>
<td>3.10.11</td>
<td>3.11.11</td>
<td>3.12.11</td>
<td>3.13.11</td>
<td>3.14.11</td>
</tr>
</tbody>
</table>

Legend:
- **Orange**: Administrative (e.g., policies, standards & procedures)
- **Light Blue**: Technical Configurations (e.g., security settings)
- **Green**: Software Solution
- **Dark Purple**: Hardware Solution
- **Software or Hardware Solution**: Software or Hardware Solution
- **Dark Brown**: Assigned Tasks To Cybersecurity Personnel
- **Dark Orange**: Assigned Tasks To IT Personnel
- **Dark Yellow**: Assigned Tasks To Application/Asset/Process Owner
- **Dark Red**: Configuration or Software Solution
- **Dark Green**: Configuration or Hardware or Outsourced Solution

Compliance Forge
CMMC Level 2
CMMC Level 3
CMMC Level 4 & 5

Implementing SP 800-171

Everything CMMC is DRAFT

CMMC Level 1

CMMC Level 2

CMMC Level 3

CMMC Level 4 & 5

?
Notes from CMMC Jan – March 2020

Standard are not yet released
NO ONE is accredited, no certified training exists, yet.
DFARS, still require self-assessments under NIST 800-171
COMPLIANCE with CMMC items cannot with certainty be issued

https://www.acq.osd.mil/cmmc/inde.html is the official DOD site for CMMC standards

When will contracts be requiring CMMC Levels?

Great question, anyone giving you a date, is providing wishful thinking at the moment,
Even purchasing agents of the government don’t know.

But an audit of your self-reported NIST 800-171 compliance could occur.

Be careful who purports to be such an auditor, and remember your information at that
level is proprietary and can be shown but should not be given, as that is like giving the
keys to your truck! Treat it the same way you should treat CUI
WHY 800-171

Customers are always asking me to comply with "new" requirements. Some seem a little silly. This one proves to be a very real threat that needs to be prevented.

"I simply can't afford to be held ransom"

Original Reason for Compliance:
  • Meet a Customer Requirement.

Revised Reason for Compliance:
  • Protect my business from cyber attacks.
Project Teamwork...

- TMAC
  - Disclaimer – TMAC is not a IT solution provider
  - TMAC specializes in assessing technical needs, developing processes & people skills.

- Company
  - Provides vision and direction
  - Commits necessary resources
  - Oversees transformation

- IT Provider
  - Assist in closing System Gaps
  - Monitor & Advise on System performance
NIST Cyber Security Framework

- Develop and implement activities to restore capabilities and maintain plans for resilience
- Develop and implement activities to take action regarding a detected event
- Develop and implement activities to identify the occurrence of a security event
- Develop an Organizational understanding to manage cyber risks to systems, people, assets, data, and capabilities
- Develop and implement safeguards to ensure delivery of critical services
Key Management Elements

Management Involvement
- Understanding Business risks & Planning
- Creating the “Sense of Urgency” for Cyber compliance
- Establishing Roles & Structure
- Providing Resources & Systems

Cyber Awareness & Communication
- Establishing a Training Program
- News Letters & Such...(Keeping up with the trends)

Site & System Security Documentation
- Digital Security Plan
- Physical Site Security Plan
- Security System Manual
- System Policies & Controls

Cyber System Checks
- Gap Assessments & Action Plans
- Periodic System Reviews
- Process Audits
- System Integrity Testing
- Culture/Behavior Testing
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Limit system access to authorized users, processes acting on the behalf of authorized users, or devices (including other systems)</td>
<td>100%</td>
<td>Does the company use passwords?</td>
<td>Yes</td>
<td>Request is made to Roland using form from Roland and submitted back to a few that are authorized to make this request.</td>
<td>No Action Req'd</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Does the company have an authentication mechanism?</td>
<td>Yes</td>
<td>For office systems, these are unique. For production, there is a single sign-on for all.</td>
<td>No Action Req'd</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Are account requests authorized before system access is granted?</td>
<td>Yes</td>
<td>Request is made to Roland using form from Roland and submitted back to a few that are authorized to make this request.</td>
<td>No Action Req'd</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Does the company maintain a list of authorized users, defining their identity and role and sync with system, application, and data layers?</td>
<td>Yes</td>
<td>Kept and maintained by Roland - Organization Master Network Privileges List</td>
<td>No Action Req'd</td>
</tr>
<tr>
<td>Limit system access to the types of transactions and functions that authorized users are permitted to execute.</td>
<td>0%</td>
<td>Do you use access control lists to limit access to applications and data based on role or identity?</td>
<td>No</td>
<td>For the office, yes, for production currently no.</td>
<td>Priorit Req'd</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Does the system allow for the separation of access control rights and enforcement of those rights?</td>
<td>No</td>
<td>For the office, yes, for production currently no.</td>
<td>Priorit Req'd</td>
</tr>
<tr>
<td>Control the flow of CUI in accordance with approved authorizations.</td>
<td>0%</td>
<td>Do you have architectural solutions to control the flow of system data?</td>
<td>No</td>
<td>For office and production currently doesn’t have in place.</td>
<td>Priorit Req'd</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Do you document Information (flow control) enforcement by using protected processing level (e.g., defensive architecture) as a basis for flow control decisions?</td>
<td>No</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Plan Of Action & Milestones

<table>
<thead>
<tr>
<th>POMM ID</th>
<th>Lead Contact</th>
<th>Priority</th>
<th>Assigned Contact</th>
<th>Task Name</th>
<th>Start Date</th>
<th>Expected Finish</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>001</td>
<td>Brandon</td>
<td>High</td>
<td></td>
<td>3.1</td>
<td>6/6/2018</td>
<td>8/31/2018</td>
<td>On Schedule</td>
</tr>
<tr>
<td>002</td>
<td>Brandon</td>
<td>High</td>
<td></td>
<td>3.4</td>
<td>6/6/2018</td>
<td>8/31/2019</td>
<td>On Schedule</td>
</tr>
<tr>
<td>003</td>
<td>Brandon</td>
<td>High</td>
<td></td>
<td>3.10</td>
<td>6/6/2018</td>
<td>10/31/2018</td>
<td>On Schedule</td>
</tr>
<tr>
<td>004</td>
<td>Brandon</td>
<td>High</td>
<td></td>
<td>Various</td>
<td>6/6/2018</td>
<td>10/31/2018</td>
<td>On Schedule</td>
</tr>
</tbody>
</table>

Priority Classification
- HIGH = MDA Priority
- Moderate = Facility level issue
- Low = Specific control level issue
Cyber Dash Board (to track progress...)
Things you can do to protect yourself at virtually NO COST
Things to do Now

- Train your employees
  - Phishing
  - Social Media
- Clean machines
  - Patches
  - Latest security software
  - Browsers
  - Operating Systems
- Use firewalls
Things to do Now

Mobile Devices
- Passwords
- Encrypt
- Install Security Apps
- Avoid Public Networks
- Report if lost or stolen
What you can do to protect yourself

- Use a strong password
  - Cracking a password requires time
  - Dictionary lists are widely available
  - Change at given intervals

Top 25 Worst Passwords of 2018

1. 123456 (rank unchanged since 2017 list)
2. password (unchanged)
3. 12345678 (up 1)
4. qwerty (up 2)
5. 123456789 (up 3)
6. hello (up 4)
7. password (unchanged)
8. 123456 (down 1)
9. password (unchanged)
10. love (down 2)

11. admin (up 1)
12. welcome (unchanged)
13. monkey (new)
14. login (changing)
15. abc123 (new)
16. starwars (new)
17. 123456789 (unchanged)
18. 12345 (unchanged)

19. password (down 1)
20. master (up 1)
21. hello (new)
22. freedom (new)
23. whatever (new)
24. qwerty (new)
25. trustno1 (new)

Dashlane
Worst Password Offenders of 2018

1. Kanye West
2. The Pentagon
3. Cryptocurrency Owners
4. Nutella
5. UK Law Firms
6. Texas
7. White House Staff
8. Google
9. United Nations
10. University of Cambridge
Things to do Now

- User Accounts for each employee
  - Strong passwords
  - Admin privileges limited
  - Admins use non-privileged accounts

- Make backups
  - Automatically
  - Weekly
  - Store offsite or in the cloud
  - Encrypted
What you can do to protect yourself

- Don’t share passwords
  - Seems simple enough, but you’d be surprised...

- One of the best tools in Social Engineering
  - “This is Bob from IT…”

Consider using a password manager
What you can do to protect yourself

- Do not use ‘found’ USB drives
  - Found could be literal, or giveaway
  - When in doubt, throw it out
What you can do to protect yourself

- **Wireless router at home and work**
  - Make sure you change the default name (SSID) of the router
  - Make sure you change the default user name and password to access the router
  - Do not have the wireless password the same as the router, use many characters
Things to do Now

- Strong Passwords
  - Change every three months
  - At least 12 characters
    - Number
    - Special character
  - Multi-factor Authentication
  - Train Employees
Things to do Now

- Secure Your Wi-Fi
  - Encrypt
  - Do not broadcast network name
    - Service Set Identifier (SSID)
  - Password protect router
  - Separate “guest” use from “business” use.
What you can do to protect yourself

- Make sure system is up-to-date on patches
  - This includes ALL software
  - If it has auto-update, click and forget it
  - Reminders can be annoying, but they are there for a reason
Things to do Now

- Payment Cards
  - Trusted and validated tools
  - Anti-fraud services
  - Isolate payment systems

- Limit Access
  - No one has access to all
  - Based on roles
  - SW Install needs permission (limited admin privileges)
From NIST SP 800-171 to CMMC

In addition to the requirements of NIST SP 800-171 you will need:

To achieve **CMM C Maturity Level 2**
- Documented Policies, Processes and Procedures for all requirements.

To achieve **CMM C Maturity Level 3**
- Introduced Asset Management, Situational Awareness and Recovery “Domains”
- Completed SSP (System Security Plan) AND documented plans for all activities.
Resources

- NIST Small Business Cybersecurity Corner


- MEP National Network Assistance
  - [www.nist.gov/mep](http://www.nist.gov/mep)

- DOD CMMC Model
  - [www.acq.osd.mil/cmmc/draft.html](http://www.acq.osd.mil/cmmc/draft.html)

- TMAC
  - [www.tmac.org](http://www.tmac.org)