Gap Analysis: Configuring Your Microsoft Office 365/Azure Environment(s) for NIST 800-171 Compliance
Updated Annually by fiscal year
2019 edition exceeded 2000 pages

Managed by:
DoD
NASA
General Services Administration
FAR has all of the basics:

Access Control
Limited Privileges
Device Auditing
Data Control
User Auditing
User Authentication
Media Disposal
Physical Access Control
Visitor Management
Communication/Boundary Control
Subnetting Internal Networks
Breach Reporting
Anti-Malware
Patch Management
Periodic System Scan/Audit

Keeps you on the hook for basic negligence
Here’s all the areas the FAR is concerned with, if they or their subcontractors receive federal funds.
By concerned with, I mean Flow Downs.

IT - NIST 800-53
Nuclear has NERC
Energy has FERC
Finance has DSS
Healthcare has HIPPA
Chemical has CFATS
Water got anew one form the EPA last year called the American Water Infrastructure Act

DHS has been around for 20 years now and we’re really starting to see that maturity

Specifically today, we’re going inside of the Defense Industrial Base, it’s likely the most evolved owing to its breadth.
DFARS – DEFENSE FEDERAL ACQUISITION REGULATION SUPPLEMENT
A supplement to the FAR that provides DoD-specific acquisition regulations that DoD government acquisition officials – and those contractors doing business with DoD – must follow in the procurement process for goods and services.
Also Defense Contract Audit Agency / DCAA

Navigating the DFARS clause is the first place that most people slip up on their implementation.

Let’s drill down into that verbiage a little bit
252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting.
As prescribed in 204.7304(c), use the following clause:

**SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING (OCT 2016)**

**c** Cyber incident reporting requirement.

(i) When the Contractor discovers a cyber incident that affects a covered contractor information system or the covered defense information residing therein, or that affects the contractor’s ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract, the Contractor shall -

   - Conduct a review for evidence of compromise of covered defense information, including, but not limited to, identifying compromised computers, servers, specific data, and user accounts. This review shall also include analyzing covered contractor information system(s) that were part of the cyber incident, as well as other information systems on the Contractor’s network(s), that may have been accessed as a result of the incident in order to identify compromised covered defense information, or that affect the Contractor’s ability to provide operationally critical support; and
   - Rapidly report cyber incidents to DoD at http://sln.net.dod.mil/

**e** Media preservation and protection. When a Contractor discovers a cyber incident has occurred, the Contractor shall preserve and protect images of all known affected information systems identified in paragraph (c)(1)(i) of this clause and all relevant monitoring/packet capture data for at least 90 days from the submission of the cyber incident report to allow DoD to request the media or decline interest.

**f** Access to additional information or equipment necessary for forensic analysis. Upon request by DoD, the Contractor shall provide DoD with access to additional information or equipment that is necessary to conduct a forensic analysis.

**g** Cyber incident damage assessment activities. If DoD elects to conduct a damage assessment, the Contracting Officer will request that the Contractor provide all of the damage assessment information gathered in accordance with paragraph (e) of this clause.

   (i) Cloud computing services shall be subject to the security requirements specified in the clause 252.239-7010, Cloud Computing Services, of this contract.

Our ref is the 252.204-7012 DFARS clause
Our problem is the Cloud Service Provider’s (CSP) environmental compliance with C and G

In Office 365 and Azure, these aren’t provided below the Microsoft Government Community (GCC) High License Level.
BTW not many CSP’s can sell you FedRAMP GCC High Licenses.
You also have to be verified (by Microsoft) as having a contract issued to you by the government before authorized CSP’s can sell you a license.

So what is this CUI anyway
Everything you need to know about CUI comes from the National Archives

History
Markings
Types of controls
Reports
Training Tools

*Note these categories aren’t limited to Defense
There are 20 Groupings currently, and over 100 CUI categories
<table>
<thead>
<tr>
<th>Category</th>
<th>Keywords</th>
</tr>
</thead>
<tbody>
<tr>
<td>Immigration</td>
<td>Asylee, Related Spouse or Child, Permanent Resident Status, Status Adjustment, Temporary Protected Status, Victims of Human Trafficking, Visa</td>
</tr>
<tr>
<td>Intelligence</td>
<td>Agriculture, Foreign Intelligence Surveillance Act, Foreign Intelligence Surveillance Act Business Records, General Intelligence, Geospatial Product Information, Intelligence Financial Records, Internal Data</td>
</tr>
<tr>
<td>International Agreements</td>
<td>International Agreement Information</td>
</tr>
<tr>
<td>Law Enforcement</td>
<td>Accident Investigation, Campaign Funds, Committed Person, Communications, Controlled Substances, Criminal History Records Information, DNA, General Law Enforcement, Informant, Investigation, Juvenile, Law Enforcement Financial Records, National Security Letter, Pre-Registration/Pre-Travel, Rewind, Sex Crime Violent, Financial Screening, Identity Theft/False Identity</td>
</tr>
<tr>
<td>Export Control</td>
<td>Export Controlled, Export Controlled Research</td>
</tr>
<tr>
<td>Statistical</td>
<td>Investment Survey, Pedestor Predictive Survey, Statistical Information, US Census</td>
</tr>
<tr>
<td>Tax</td>
<td>Federal Taxpayer Information, Tax Correction, Taxpayer Advocate Information, Written Determinations</td>
</tr>
<tr>
<td>Transportation</td>
<td>External Safety Analysis Records, Sensitive Security Information</td>
</tr>
</tbody>
</table>
As CUI pertains to the Defense Sector and the Electronic Security Industry

Research and Engineering Data (Site Survey docs)
Engineering Drawings (System Connectivity and Equipment Location diagrams)
Associated lists (IP Address info), Specifications (Throughput, Storage, Encryption)
Software code and source code (publicly available doesn’t count)

All right so now we know what the information is.
So if we’re gonna use O365 and Azure to process and store CUI, we’ve got to meet the FAR and DFARS guidance.

How do we do that?
Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

RON ROSS
PATRICK VISCUSO
GARY GUSSANIE
KELLEY DEMPSEY
MARK RIDDLE

First published in June 2015 and then retracted, Latest revision is from Nov 2017
Went live with self attestation in Dec 2018, 77 pages
So for each family you will have 110 technical or non-technical controls and sub-controls that must be implemented, monitored, automated, and reported upon. Oh and don’t forget you’ll need the policies that drive them.

There are some free tools for measuring your cyber maturity like the Center for Internet Security’ CSAT tool, and its free

Check it out if you’re struggling for a good documentation tool. Today you’re gonna see how its done in the Microsoft environment as well

For ease of use, the security requirements are organized into fourteen families. Each family contains the requirements related to the general security topic of the family. The families are closely aligned with the minimum security requirements for federal information and information systems described in FIPS Publication 200. The contingency planning, system and services acquisition, and planning requirements are not included within the scope of this publication due to the aforementioned tailoring criteria. Table 1 lists the security requirement families addressed in this publication.

<table>
<thead>
<tr>
<th>FAMILY</th>
<th>FAMILY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control</td>
<td>Media Protection</td>
</tr>
<tr>
<td>Awareness and Training</td>
<td>Personnel Security</td>
</tr>
<tr>
<td>Audit and Accountability</td>
<td>Physical Protection</td>
</tr>
<tr>
<td>Configuration Management</td>
<td>Risk Assessment</td>
</tr>
<tr>
<td>Identification and Authentication</td>
<td>Security Assessment</td>
</tr>
<tr>
<td>Incident Response</td>
<td>System and Communications Protection</td>
</tr>
<tr>
<td>Maintenance</td>
<td>System and Information Integrity</td>
</tr>
</tbody>
</table>

TABLE 1: SECURITY REQUIREMENT FAMILIES
So these are the types of controls you’ll see.
This also shows the NIST 800-171 mappings that derive from the much broader NIST 800-53 control set which the federal government uses.

PSA has this mapping tool free for download for its members.
Once you really dig in, you’ll come to the realization that you can do this alone if you have the chops, or use a FedRAMP compliant CSP

The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

FedRAMP enables Agencies to rapidly adapt from old, insecure legacy IT to mission-enabling, secure, and cost effective cloud-based IT.
FedRAMP created and manages a core set of processes to ensure effective, repeatable cloud security for the government. FedRAMP established a mature marketplace to increase utilization and familiarity with cloud services while facilitating collaboration across government through open exchanges of lessons learned, use cases, and tactical solutions.

Defense Information Systems Agency (DISA) is a combat support agency of the Department of Defense (DoD). The agency is composed of more than 8,000 military and civilian employees. The agency provides, operates, and assures command and

<table>
<thead>
<tr>
<th></th>
<th>Office 365 GCC</th>
<th>Office 365 GCC High</th>
<th>Office 365 GCC High DoD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Access</td>
<td>Gov’t/Contractors</td>
<td>Gov’t/Contractors</td>
<td>DoD Agencies</td>
</tr>
<tr>
<td>FedRAMP Level</td>
<td>Moderate</td>
<td>Moderate</td>
<td>Moderate</td>
</tr>
<tr>
<td>DISA Approval</td>
<td>Level 2</td>
<td>Level 4</td>
<td>Level 5</td>
</tr>
<tr>
<td>ITAR Capable</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>800-171 Capable</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>DFARS C-G Capable</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

- GCC High can be fully DFARS compliant with proper licensing, design, configuration, and policy controls
- All contractors must be Microsoft approved as having a verified need
- Some capabilities available in Office 365
- Requires a minimum of 500 licenses
control and information-sharing capabilities and a globally accessible enterprise information infrastructure in direct support to joint warfighters, national level leaders, and other mission and coalition partners across the full spectrum of military operations.

**ITAR** (International Traffic in Arms Regulations) and the EAR (Export Administration Regulations) are export control regulations run by different departments of the US Government. Both of them are designed to help ensure that defense related technology does not get into the wrong hands.

Minimum requirement has been rescinded.

50 seats 25k, environment setup, 40k, data import depends on data volume, monthly costs about 5% above GCC standard.

Good news is 65 of your technical controls will be 100% addressed. Your CSP’s audit document will satisfy the governments audit for those controls.
CoalFire is an Accredited FedRAMP 3rd Party Assessment Organization that continuously audits Microsoft and its GCC CSP’s.

This is an example of the letter you will include with the System Security Plan you submit to the Contracting Officer.
The whole point of FEDRAMP is to reuse certified system to lower cost for everyone, and in theory assure the same risk-based levels of cyber protection commensurate with the governments CUI requirements.
CUI Requirements Origin

• Federal Information Processing Standards (FIPS)
  • FIPS-200 Minimum Security Requirements for Federal Information and Information Systems

• National Institute for Standards and Technology (NIST)
  • NIST sp800-53 “Moderate Impact” security control baseline

Websites with information regarding:

Derived requirements referenced from NIST sp800-171 pg. “iv”, par. 2.
NIST sp800-171 implementation

• 800-171 requirements tailored to eliminate:
  • Uniquely Federal Requirements
    • (i.e., primarily the responsibility of the federal government)
    • (i.e., NIST sp800-53)
  • Not directly related to protecting the confidentiality of CUI
  • Expected to be routinely satisfied by non-federal organizations without specification

800-171 tailored requirements referenced from NIST sp800-171 Chapter 1, pg. 3.
NIST sp800-171 for contracts w/ US-Fed

- Applies to all components of nonfederal systems and organizations
  - that process, store, or transmit CUI, or that provide security protection for such components
  - Intended for use by federal agencies in contractual vehicles or other agreements established between those agencies and nonfederal organizations
- Broken down by 14 security families containing:
  - 110 basic requirements - from FIPS-200
  - 79 derived requirements - from NIST sp800-53

Applicability of 800-171 requirements referenced from NIST sp800-171 Chapter 3, pg. 8, “THE MEANING OF ORGANIZATIONAL SYSTEMS “
Balance Your Organization

- Balance is the Key
  - DFARS, FIPS, NIST require confidentiality
    - Focused on protecting the confidentiality of CUI
    - That's only one part of the CIA triad (confidentiality, integrity, availability)
- Don’t forget about your business objectives!
  - Integrity and Availability remain a high priority
- Create the Culture / Train Everyone
  - Everyone in the organization needs to know how to defend against malicious activity

Integrity and Availability importance referenced from NIST sp800-171 pg. “iv”, par. 2.

This is a team effort! An organization must employ a “hive mentality” to ensure the safety of people and data.

If everyone on the team is trained and vigilant, the organization’s threat landscape approaches its smallest area.
Checking Boxes vs. Creating a Culture

• Satisfying requirements does not make you secure
• Implementing, and regularly auditing, requirements creates a secure system
  • Create plans / test those plans (i.e. backups, disaster recovery)
  • Create teams / update those teams (i.e. incident response, training)
  • Create rules / enforce rules (i.e. firewall rules, password complexity)

Simply creating a System Security Plan (SSP) to attain a Fed. contract does not protect your organization or the CUI.

If you never test your backups, how do you know they will work or have not been compromised?

Attrition creates vacancies in critical teams. Reviewing these plans regularly ensures success when they’re needed.

If you don’t enforce a security policy, its of no use and provides no benefit.
CMMC Certification

• NIST sp800-171B will be published in the next few months
  • Will include Cyber-Security Maturity Model Certification (CMMC)
  • Builds on DFARS 252.204-7012
• All organizations must be certified and assigned a level (1-5)
  • Beginning Jan 2020, all new contracts will require CMMC level
  • The required CMMC level will be contained in the RFP sections L & M
  • Will be a “go/no go decision” decision”
  • To be included in RFIs (June 2020) and new Solicitations (Late 2020)
  • Existing contracts can be certified

Referenced from The Office of the Under Secretary of Defense for Acquisition & Sustainment

Cybersecurity Maturity Model Certification (CMMC):

### CMMC Levels

<table>
<thead>
<tr>
<th>Level</th>
<th>Initial Thinking</th>
<th>Updated Mapping of NIST SP 800-171 rev1</th>
<th>Initial Mapping of Draft NIST SP 800-171 revB</th>
</tr>
</thead>
<tbody>
<tr>
<td>CMMC Level 5</td>
<td>Advanced / Progressive</td>
<td>4 security controls</td>
<td></td>
</tr>
<tr>
<td>CMMC Level 4</td>
<td>Proactive</td>
<td>26 security controls</td>
<td></td>
</tr>
<tr>
<td>CMMC Level 3</td>
<td>Good Cyber Hygiene</td>
<td>47 security controls</td>
<td></td>
</tr>
<tr>
<td>CMMC Level 2</td>
<td>Intermediate Cyber Hygiene</td>
<td>46 security controls</td>
<td></td>
</tr>
<tr>
<td>CMMC Level 1</td>
<td>Basic Cyber Hygiene</td>
<td>17 security controls</td>
<td></td>
</tr>
</tbody>
</table>

Office of the Under Secretary of Defense for Acquisition & Sustainment

Office 365 / Azure & NIST/DFARS

• Can I use Office 365 / Azure if I must comply with DFARS / NIST?
  • Yes. However, you must choose the correct level of service.

• Office 365 is certified
  • to the objectives specified in the NIST Cyber Security Framework (CSF)

• Microsoft Cloud services
  • Have undergone independent, third-party FedRAMP Moderate and High Baseline audits
  • Are certified according to the FedRAMP standards

Your organizational needs will guide you to choose the correct Office 365 / Azure level of service.
Office 365 & NIST/DFARS (cont)

• Office 365 & Office 365 GCC
  • NIST 800-171 CMMC capable up to level 3
• Office 365 GCC High
  • NIST 800-171, DFARS C-G capable
• Services in scope for GCC and GCC High
  • Access Online, Azure Active Directory, Exchange Online, Exchange Online Protection, Office 365 ProPlus, Office Delve, Office Online, OneDrive for Business, Project Online, SharePoint Online, Skype for Business

DFARS C-G requires that physical hard drives be turned over to the Federal Govt. should a cyber incident occur.

Only Office 365 GCC High offers this service.

For any DFARS contracts, organizations wishing to use Office 365 / Azure must choose GCC High.
Shared NIST 800-171 Controls in Office 365

- When operating in a cloud environment, there are “shared” controls
  - *example 1*: Identification and Authentication
    - cntl IA 3.5.3: multi-factor authentication (MFA) for privileged accounts
    - your org. must implement, cloud vendor will certify their controls
  - *example 2*: Awareness and Training
    - cntl AT 3.2.1: Security Awareness Training
    - your org. must implement, cloud vendor will certify their program

These are examples of controls that must be implemented in your cloud hosting environment AND any/all non-cloud organizational environments.
Office 365 Compliance Manager

- Security Compliance and governance
  - https://servicetrust.microsoft.com/ComplianceManager

These tools are for contractors wishing to be compliant with NIST 800-171 but not requiring DFARS relating services.

Compliance Manager:
https://servicetrust.microsoft.com/ComplianceManager
- GCC High has more advanced tools.
Office 365 NIST 800-171 assessments

• NIST 800-171 compliance config. for Office 365 Gov plans only.
• Can still add to regular plans
  • as “assessment”

These tools are for contractors wishing to be compliant with NIST 800-171 but not requiring DFARS relating services.

Compliance Manager:
https://servicetrust.microsoft.com/ComplianceManager
- GCC High has more advanced tools.
In-Scope Controls Assessment

- Shared controls management in Compliance Manager

This control panel is from an Office 365 non-government plan.

Easy to use tools for NIST 800-171 assessment and governance.
### Detailed Controls Breakdown

**• Multi-Factor Authentication (MFA) Requirements**

This control panel is from an Office 365 non-government plan.

Easy to use tools for NIST 800-171 assessment and governance.

Screen shot show drill-down to related controls.
Reporting Tool

• Assessment Reporting Tool

This control panel is from an Office 365 non-government plan.

Easy to use tools for NIST 800-171 assessment and governance.

Screen shot shows the reporting tool with export to MS Excel.