Left Brain Professionals

Compliance ★ Government Contracts ★ Accounting

Cybersecurity Compliance in Government Contracts

Robert E. Jones

CPA, CPCM, NCMA Fellow

DyNet

Dynamic Networking for Small Business

Left Brain Professionals

Positive Share

“You don’t have to be great to start, but you have to start to be great.”

~ Zig Ziglar

Left Brain Professionals

Safety Check

Left Brain Professionals

FAR Rule

52.204-21 Basic Safeguarding of Covered Contractor Information System

15 items "a prudent business person would employ…even if not covered by this rule."

Left Brain Professionals

DFARS Rule

DFARS 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting

Note the “Cyber Incident Reporting”

Requires compliance with NIST (SP) 800-171

Left Brain Professionals

Controlled Unclassified Info (CUI)

115 categories and subcategories

Controlled Defense Information (CDI)

Controlled Technical Information (CTI)

Left Brain Professionals

NIST (SP) 800-171 R1

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

110 items across 14 categories of controls

Performance based requirements

One Size Fits All!

There are no scaled solutions for NIST 800-171

While some items may not apply to some entities, the general requirement remains.

Left Brain Professionals

Internal Assessment

Do you process, store, or transmit CUI through your network or systems?

Identify all data

Identify all networks, software, and apps

Review policies & procedures

Left Brain Professionals

Internal Assessment - Data

What kind of data do you process, store, or transmit?

CDI/CTI – Controlled Defense/Technical Information

PII – Personally Identifiable Information

PHI – Personal Health Information

Other

Internal Assessment - System

Where/how is it processed, stored, or transmitted?

Internal network

Cloud

Apps

Left Brain Professionals

Internal Assessment - Policies

Do you have written policies & procedures?

Configuration management

Access control & authorization

Physical access

Maintenance

Internal Assessment

Excel list of the NIST 800-171 requirements as a starting point.

Yes – with links or references

No – with info for the POA&M

N/A – document why N/A

Hiring External Help

Technical firms – focus on the technical aspects of installation and configuration

Consulting firms – focused on compliance

CPA firms – focused on audits and compliance

System Security Plan (SSP)

An overview of the security requirements of the system and description of the controls in place or planned, responsibilities and expected behavior of all individuals who access the system.

Plan of Actions & Milestones (POA&M)

Document to assist organizations in identifying, prioritizing, and monitoring the progress of corrective efforts for security weaknesses/deficiencies/vulnerabilities found in programs and systems.

Left Brain Professionals

External Reviews & Audits

DoD not accepting third-party verification

Q25: Will the DoD certify that a contractor is 100% compliant with NIST SP 800-171? Is a 3rd Party assessment of compliance required?

A25: No new oversight paradigm is created through this rule. If oversight related to these requirements is deemed necessary, it can be accomplished through existing FAR and DFARS allowances, or an additional requirement can be added to the terms of the contract. The rule does not require "certification" of any kind, either by DoD or any other firm professing to provide compliance, assessment, or certification services for DoD or Federal contractors. Nor
will DoD give any credence to 3rd party assessments or certifications – by signing the contract, the contractor agrees to comply with the terms of the contract. It is up to the contractor to determine that their systems meet the requirements.

Some companies with limited cybersecurity expertise may choose to seek outside assistance in determining how best to meet and implement the NIST SP 800-171 requirements in their company. But, once the company has implemented the requirements, there is no need to have a separate entity assess or certify that the company is compliant with NIST SP 800-171.

Primes may require third-party verification of subs

Left Brain Professionals

Cybersecurity in GovCon Acquisition

Government may request SSP and/or POA&M as part of RFP

May identify cybersecurity compliance as an evaluation factor

Left Brain Professionals

Gov’t Ensuring Compliance

Evaluating SSP as part of the solicitation

Q21: How can DoD consider an offeror’s compliance with NIST SP 800-171 in the source selection process?

A21: The intent of DFARS clause 252.204-7012 is to ensure that the security requirements in NIST SP 800-171 are applied to information systems that are owned by, or operated by or for contractors, and process, store, or transmit CDI. The clause is not structured to require contractor compliance with NIST SP 800-171 as a mandatory evaluation factor in the source selection process, but the requiring activity is not precluded from stating in the solicitation that it will consider compliance with NIST SP 800-171 in the source selection process. Examples of how a requiring activity might proceed include:

- Notifying the offeror that its approach to protecting covered defense information and providing adequate security in accordance with DFARS 252.204-7012 will be evaluated in the solicitation on an acceptable or unacceptable basis. Proposal instructions and corresponding evaluation specifics of what constitutes acceptable/unacceptable compliance with NIST SP 800-171 must be detailed in sections L and M of the solicitation as well as the Source Selection Plan.

- Establishing compliance with DFARS 252.204-7012 as a separate technical evaluation factor and notifying the offeror that its approach to providing adequate security will be evaluated in the source selection process. The specifics of how offeror compliance with NIST SP 800-171, will be evaluated must be detailed in Sections L and M of the solicitation as well as the Source Selection Plan.

Left Brain Professionals

Gov’t Ensuring Compliance

Making the POA&M part of contract oversight.

Tying progress reports and milestone payments to the POA&M.

Left Brain Professionals

Cost of Non-Compliance

What if you don’t complete the POA&M tasks on time?

You may not get paid!

Left Brain Professionals

Cost of Non-Compliance

What if the SSP is not solid or complete?

You may not win the award!

Cost of Non-Compliance

Liquidated damages for late delivery or non-conforming data.

Left Brain Professionals

Cost of Non-Compliance

What if you deliver non-conforming data?

You may not get paid!

Left Brain Professionals

Failure to Properly Mark CUI

I believe this will be the number one failure point for many companies.

Left Brain Professionals

Cost of Non-Compliance

Cure notices

Stop work orders

Terminations

Poor performance rating in CPAR

Left Brain Professionals

Compliance Strategies

Other frameworks

SANS/CIS 20

COBIT 5

ISO/IEC 27001

Sarbanes-Oxley*

*Mandatory for public issuers

Compliance Strategies

Rely on the cloud

Scalable
Affordable
Secure
Reliable

Know where your data is stored!

Left Brain Professionals

Compliance Strategies

Office 365 over Google

Google

Google Data Centers

Search this site

Data centers › Inside look › Locations

Data center locations

We own and operate data centers around the world to keep our products running 24 hours a day, 7 days a week. Find out more about our data center locations, community involvement, and job opportunities in our locations around the world.

Americas

Berkeley County, South Carolina
Council Bluffs, Iowa
Douglas County, Georgia
Jackson County, Alabama
Lenoir, North Carolina
Mayes County, Oklahoma
Montgomery County, Tennessee
Quilicura, Chile
The Dalles, Oregon

Asia

Changhua County, Taiwan
Singapore

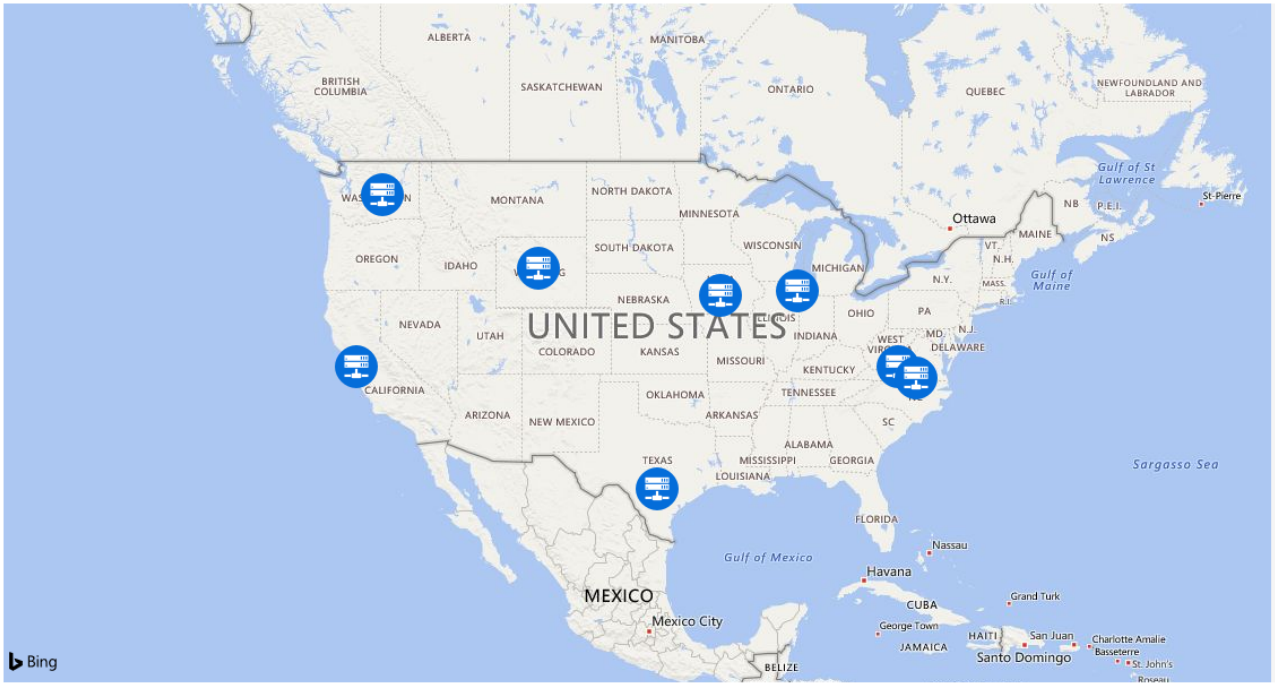
Europe

Dublin, Ireland
Eemshaven, Netherlands
Hamina, Finland
St Ghislain, Belgium

Left Brain Professionals

Office 365

North America



Location of customer data at rest

Quincy, WA
Chicago, IL
San Antonio, TX
Des Moines, IA
Blue Ridge, VA
Cheyenne, WY

Azure Active Directory

Boydton, VA
San Jose, CA

Azure Active Directory
Dynamics 365

- Sales
- Customer Service
- Field Service
- Project Service Automation

This data map describes where Microsoft stores customer data in the course of providing Dynamics 365 services for customers located in **North America**. Specifically, this map provides information regarding the locations of all datacenters and corresponding services for customer data stored in Dynamics 365 services in **North America**.

Microsoft replicates customer data in at least two datacenters at any given time for reliability and availability.

Left Brain Professionals

Compliance Strategies

Start with good personal cyber hygiene

Start with simple tools

Left Brain Professionals

Path Forward

Continuous process – not a “once and done.”

Train employees

Stay current

What's Next?

Expect the DFARS rule to become the FAR rule.

(Or something very similar)

Not all agencies have rules or even follow the FAR.

Left Brain Professionals

What's Next?

Protests

Cyber Incidents/Breaches

Court Cases

Contact

Robert E. Jones, CPA, CPCM, NCMA Fellow

(614) 556-4415

robert@leftbrainpro.com


AGENCY
SYSTEMS ★ PROCEDURES
LICENSING ★ CUSTOMER
REGISTRATION ★ AUDITS
POLICIES
FPO

FAR Rule

1. Limit system access to authorized users
2. Limit system access to authorized types of transactions
3. Limit connections to external systems
4. Control publicly accessible information
5. Identify system users and processes

FAR Rule

6. Authenticate users
7. Sanitize or destroy media before disposal
8. Limit physical access
9. Escort visitors and monitor activity
10. Monitor communications at external boundaries

FAR Rule

11. Separate publicly accessible systems
12. Identify and correct system flaws
13. Protect against malicious code
14. Update malicious code protections
15. Perform periodic system scans

Left Brain Professionals

NIST (SP) 800-171 R1

1. Access Control
2. Awareness & Training
3. Audit & Accountability
4. Configuration Management
5. Identification & Authentication
6. Incident Response
7. Maintenance

Left Brain Professionals

NIST (SP) 800-171 R1

8. Media Protection
9. Personnel Security
10. Physical Protection
11. Risk Assessment
12. Security Assessment
13. System & Communication Protection
14. System & Information Integrity

Left Brain Professionals

Surveys, Reviews, & Audits

Survey – consulting engagement with no assurance ($)

Review – more formal with limited assurance ($$)

Audit – most formal (and intense) with assurance ($$$)