Comparing NIST SP 800-53 R5 vs FedRAMP R5 vs NIST SP 800-171 R2 vs NIST SP 800-171 R3 IPD

Version 2023.1

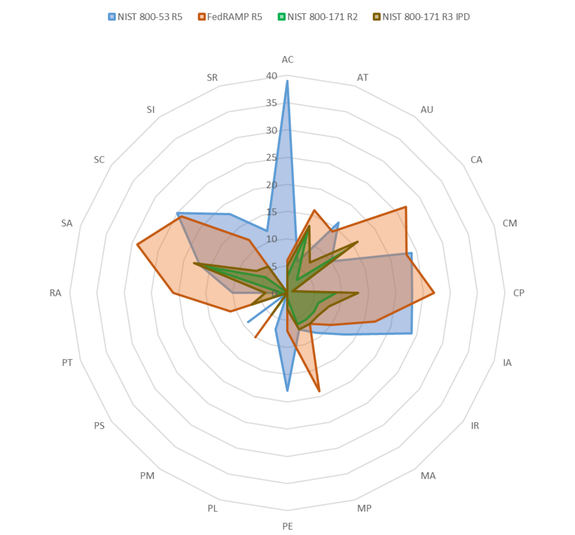
Within the Defense Industrial Base (DIB), there is considerable confusion about the concept of "FedRAMP equivalency" as it pertains to Cloud Service Providers (CSP) offerings. The purpose of the informational graphics shown below is to provide a comparison between the common frameworks relied upon by the DIB, specifically NIST SP 800-53 R5, FedRAMP R5, NIST SP 800-171 R2 and the Initial Public Draft (IPD) of NIST SP 800-171 R3. For the DIB, the discussion really begins around Federal Information Processing Standards (FIPS) 199 and 200, since that is what sets the stage for utilizing the NIST SP 800-53 moderate baseline as a starting point to protect Controlled Unclassified Information (CUI). This concept is shown in greater detail on the second page of this document, but the summary concept is:

- When you follow the footnote to the bottom of **page 5 of NIST SP 800-171 rev2**, it states *"the moderate impact value defined in [FIPS 199] may become part of a moderate impact system in [FIPS 200], which requires the use of the moderate baseline in [SP 800-53] as the starting point for tailoring actions."*
- From **page 4 of FIPS 199**, it states *"…the potential impact values assigned to the respective security objectives (confidentiality, integrity, availability) shall be the highest values (i.e., high water mark) from among those security categories that have been determined for each type of information resident..."*
- From **DFARS 252.204-7012(2)(ii)(D)**, this is where "FedRAMP equivalency" is stated: *"...meets security requirements equivalent to those established by ... FedRAMP Moderate baseline."*

The most important take-aways from this document should be:

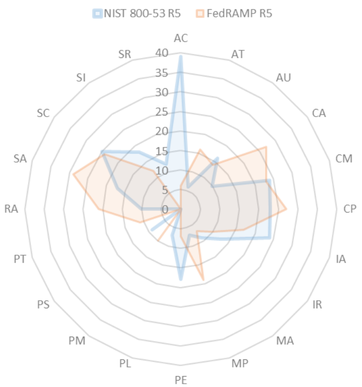
- FedRAMP R5 (moderate) ≠ NIST SP 800-53 R5 (moderate) | FedRAMP R5 (moderate) > NIST SP 800-53 R5 (moderate)
- FedRAMP R5 (moderate) ≠ NIST SP 800-171 R2 or R3 IPD | FedRAMP R5 (moderate) > NIST SP 800-171 R2 or R3 IPD
- FedRAMP R5 (moderate) ≠ CMMC 2.0 Level 2 | FedRAMP R5 (moderate) > CMMC 2.0 Level 2

NIST SP 800-53 R5 vs FedRAMP R5 vs NIST SP 800-171 R2 vs NIST SP 800-171 R3 IPD



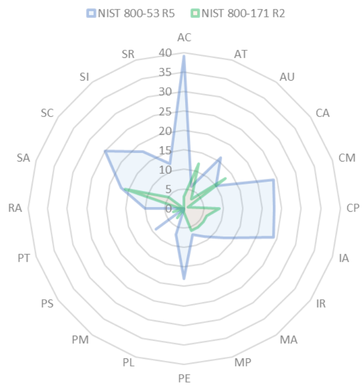
NIST 800-53 R5 Control Family	Identifier	NIST 800-53 R5	FedRAMP R5	NIST 800-171 R2	NIST 800-171 R3 IPD
Access Control	AC	39	6	3	5
Awareness & Training	AT	6	16	12	13
Audit & Accountability	AU	16	14	3	7
Assessment, Authorization & Monitoring	CA	10	27	13	16
Configuration Management	CM	24	23	1	1
Contingency Planning	CP	23	27	9	13
Identification & Authentication	IA	24	17	6	8
Incident Response	IR	13	10	6	7
Maintenance	MA	9	7	6	7
Media Protection	MP	7	19	6	7
Physical & Environmental Protection	PE	18	7	1	3
Planning	PL	7	0	0	0
Program Management	PM	0	10	3	5
Personnel Security	PS	9	0	0	0
Personally Identifiable Information (PII) Processing & Transparency	PT	0	11	3	7
Risk Assessment	RA	10	21	1	4
System & Services Acquisition	SA	17	29	16	18
System & Communications Protection	SC	25	24	5	7
System & Information Integrity	SI	18	12	0	6
Supply Chain Risk Management	SR	12	0	0	0

NIST SP 800-53 R5 vs FedRAMP R5



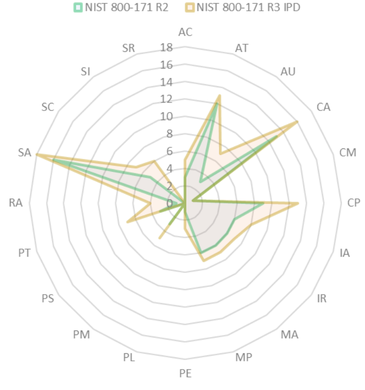
Identifier	NIST 800-53 R5	FedRAMP R5
AC	39	6
AT	6	16
AU	16	14
CA	10	27
CM	24	23
CP	23	27
IA	24	17
IR	13	10
MA	9	7
MP	7	19
PE	18	7
PL	7	0
PM	0	10
PS	9	0
PT	0	11
RA	10	21
SA	17	29
SC	25	24
SI	18	12
SR	12	0

NIST SP 800-53 R5 vs NIST SP 800-171 R2



Identifier	NIST 800-53 R5	NIST 800-171 R2
AC	39	3
AT	6	12
AU	16	3
CA	10	13
CM	24	1
CP	23	9
IA	24	6
IR	13	6
MA	9	6
MP	7	6
PE	18	1
PL	7	0
PM	0	3
PS	9	0
PT	0	3
RA	10	1
SA	17	16
SC	25	5
SI	18	0
SR	12	0

NIST SP 800-171 R2 vs NIST SP 800-171 R3 IPD



Identifier	NIST 800-171 R2	NIST 800-171 R3 IPD
AC	3	5
AT	12	13
AU	3	7
CA	13	16
CM	1	1
CP	9	13
IA	6	8
IR	6	7
MA	6	7
MP	6	7
PE	1	3
PL	0	0
PM	3	5
PS	0	0
PT	3	7
RA	1	4
SA	16	18
SC	5	7
SI	0	6
SR	0	0

ITAR vs EAR vs DFARS vs FAR: Minimum Cybersecurity Requirements

ITAR

22 CFR Parts 120-130

EAR

15 CFR Parts 730-774

DFARS

252.204-7012

FAR

52.204-21

May be categorized as

CUI must adhere to

CUI CATEGORY

CUI // SP-EXPT

Must adhere to

CUI PROGRAM

CUI NOTICE 2020-04

NIST FIPS PUB 199

SECURITY CATEGORIZATION

CONFIDENTIALITY = MODERATE

Establishes CUI as MODERATE confidentiality

NIST FIPS PUB 200

SECURITY IMPACT LEVEL

IMPACT = MODERATE

Establishes CUI as MODERATE impact

NIST SP 800-53

NIST SP 800-53 CONTROLS

MODERATE BASELINE

[high water mark of FIPS 199 & 200]

Specifies

Is further tailored to address CUI-specific protection

NIST SP 800-171

NIST SP 800-171 TAILORING

CUI, NFO, NCO & FED CONTROLS

NFO controls would be assess by

Specifies

CUI controls would be assessed by

NIST SP 800-171A

ASSESSMENT OBJECTIVES

CUI CONTROLS

NIST SP 800-53A

ASSESSMENT OBJECTIVES

NFO CONTROLS

Provides Evidence To Address

COMPLIANCE FORGE

www.ComplianceForge.com

version 2023.1