# DFARS Cybersecurity for Fiscal Year 2024: Keeping up with a moving target

Note: This whitepaper provides additional documentation for topics covered in the 8-minute video "DFARS Cybersecurity FY 2024 Updates".

## Overview:

With the finalization of DFARS 252.204-7024 Contract Officers are now REQUIRED to consider SPRS scores, where available, in contract awards.

## DCMA Audit Experience

The DCMA has conducted more than 100 audits over the last 18 months. The results of their audits are summarized below, with a listing of the top 3 Other Than Satisfied (OTS) items.

1) 3.13.11, FIPS-validated cryptography
2) 3.5.3, Multifactor Authentication
3) 3.14.1, Identify, report, correct system flaws

Each of these items will be discussed separately.

## FIPS validated cryptography

FIPS validated cryptography (link) has over 900 modules that are currently FIPS validated. Validations are typically good for 5 years unless revoked. Some modules are firmware (38), 425 are software or software hybrid, one is a hardware/firmware hybrid and 464 are hardware.

Most vendors have multiple certifications. For example, Fortinet (an ACR 2 investor) has 66 validated modules, 42 of which are "historical" and usable only in existing systems. Almost 3000 modules have been validated since the start of the program. A list of vendors is here.

The FIPS validation program admits to a significant backlog. The NIST lists 275 modules on their "Modules in Process" list. This is a serious problem for suppliers who frequently update their product lines, since their validated products may not be part of their current product line.

Data at rest modules are validated for McAffee, Western Digital, Apple, Microsoft and others. Data in motion modules are validated for Fortinet, SonicWall, Cisco and others. Data at rest and data in motion validated modules are available from Hewlett Packard, Juniper, and others.

Finding a validated module for small business use can be challenging, which is probably why CUI 3.13.11, use of FIPS validated cryptography, is the #1 missing item on most DCMA audits. Most FIPS validated products are aimed at the federal market, where FIPS validation is mandatory.

There are a few small business appropriate products available. Microsoft BitLocker (certificate 4461) is a popular choice for Windows™ users. The SonicWall TZ270 (certificate 4162) is recommended for 1-10 users. The unit is $840 with a one year license at Firewalls.com. The validated Western Digital self-encrypting 7.68 tb hard drive (certificate 4309) is $450 online.

FIPS validated cryptography products are a very tiny fraction of the products available. Meeting this requirement will be very challenging for many contractors.

## Multi-Factor Authentication

Multi-Factor Authentication (MFA) requires additional proof of identity beyond, or sometimes in place of, username and password. The three types of MFA are

1. Things you know (knowledge).
2. Things you have (possession).
3. Things you are (inherence).

Dongles and biometric based MFA are common. Fingerprint identification is now a typical feature for laptop computers. Add-on fingerprint scanners are available for as little as $16. However, probably the most common MFA approach is the one-time code sent to phone, text (not recommended), or email.

PC Magazine's 2023 review article notes a number of phone based MFA options from Google, Duo, Microsoft and 2FAS. These apps allow MFA access to online accounts and are typically free. Duo also allows MFA access to Windows™ logon in either the free or paid versions. Other local machine options are available.

## Timely Detecting and Correcting System Flaws

Complying with DFARS 252.204-7012 is not easy. A fully compliant site will satisfy 110 requirements of NIST 800-171 rev. 2, as documented in a System Security Plan or SSP. Each of the 110 requirements has a point score of 1, 3, or 5 points, since not all precautions are equally important. SSP scores range from 110 at full compliance down to -203. Average DoD contractor scores reported in the 2022 Cyberoam survey, for the 44% of contractors who reported scores, were -23.

Achieving 110-point compliance is a major achievement, and the temptation is to stop working and celebrate. That is not a good idea.

If your initial score is 110, and you do none of the 4 daily tasks, tomorrow your score will drop from 110 to 88.

If you don't do the 5 weekly tasks, your score drops to 53.

And if you neglect the monthly and quarterly tasks, your score drops to -20, which is where you were a year ago.

Safety controls have a limited shelf life. All safeguards need to be reviewed annually. A few safeguards need to be checked daily. While this need not be time consuming, you need to lock the door and set the alarm EVERY DAY. If you wouldn't leave your doors unlocked, why would you leave your network unprotected?

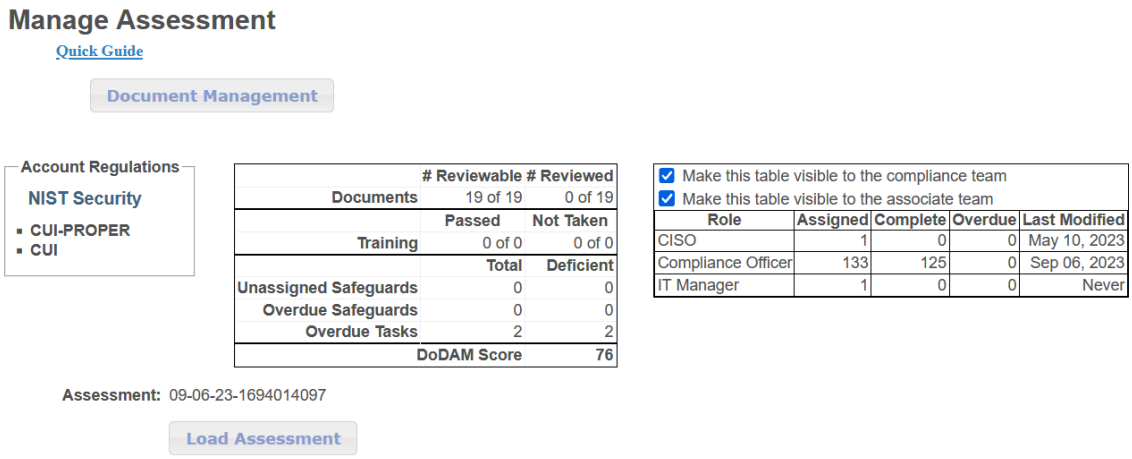
To accommodate the updated safeguards frequency, 16 of the 87 policy templates have been updated, as listed on the following page..

| | |
|---|---|
| CUI 3.1.22 | CUI 3.4.5 |
| CUI 3.1.7 | CUI 3.10.1 3.10.2 |
| CUI 3.3.1 3.3.2 | CUI 3.11.1 |
| CUI 3.3.5 | CUI 3.11.2 |
| CUI 3.3.6 | CUI 3.12.1 3.12.2 3.12.3 3.12.4 |
| CUI 3.3.9 | CUI 3.14.1 3.14.2 3.14.3 |
| CUI 3.4.1 3.4.2 | CUI 3.14.4 3.14.5 |
| CUI 3.4.3 | CUI 3.14.6 |

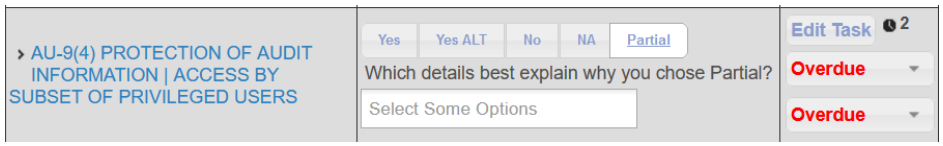
If you have not received your updated policy templates, contact sales@acr2solutions.com.

## Demonstration of Updating Procedure

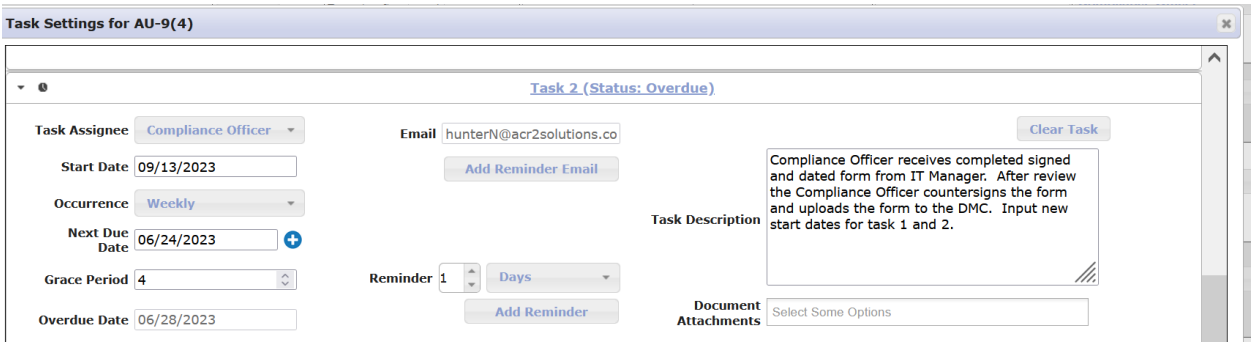
**Site:** Bobby Lee Welding is a fictional demonstration site. In the example shown, safeguard AU-9(4) had been allowed to go overdue, setting the safeguard status from “Yes” to “Partial”. The DoD Assessment or DoDAM score is a respectable 76, as shown on the following below.



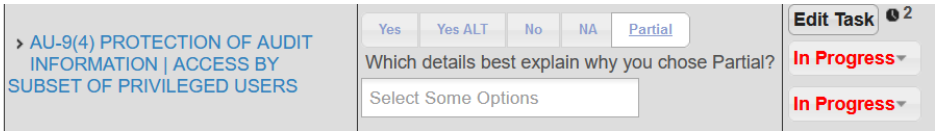

NIST 800-53 safeguard has two overdue tasks, shown in red below.



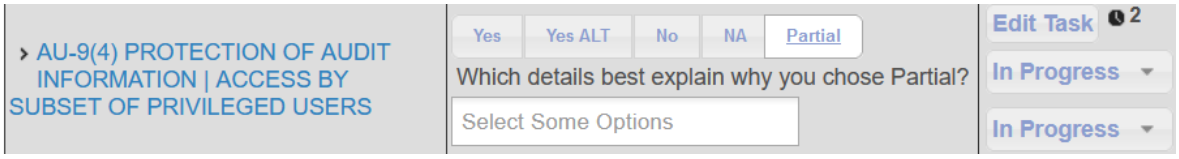

Detailed task dates are shown below for Task 2. Overdue date is 6/28/2023 and status is “Overdue”




Inputting new start dates for both tasks gets a status change to “**In Progress**”, as shown below.




Hitting “Submit and Finalize” removes the red color.




Safeguard status is still listed as “Partial” and the DoDAM score remains at 76. Manually resetting status to yes, you can then “Submit and Finalize” to update the score to 78, as shown on the below.

Quick Guide

Document Management

**Account Regulations**

**NIST Security**

- CUI-PROPER
- CUI

| | # Reviewable | # Reviewed |
|---|---|---|
| Documents | 19 of 19 | 0 of 19 |
| | Passed | Not Taken |
| Training | 0 of 0 | 0 of 0 |
| | Total | Deficient |
| Unassigned Safeguards | 0 | 0 |
| Overdue Safeguards | 0 | 0 |
| Overdue Tasks | 0 | 0 |
| DoDAM Score | | 78 |

☑ Make this table visible to the compliance team
☑ Make this table visible to the associate team

| Role | Assigned | Complete | Overdue | Last Modified |
|---|---|---|---|---|
| CISO | 1 | 0 | 0 | May 10, 2023 |
| Compliance Officer | 133 | 127 | 0 | Sep 06, 2023 |
| IT Manager | 1 | 0 | 0 | Never |