ACR 2 Cybersecurity Risk Management System (ACRMS™) Update for Fiscal Year 2022

Welcome to the fiscal year 2022 update of the ACR 2 Cybersecurity Risk Management System or ACRMS™. Developed in 2018 for Air Force contractors as a three day DFARS cybersecurity policy Boot Camp, the self-paced video-enhanced ACRMS™ is periodically updated to reflect changes in Federal guidance. As we all know, DFARS cybersecurity is a moving target.

The current iteration of the ACRMS combines video-enhanced policy creation templates with automated NIST 800-30 risk assessment and an extensive task management, documentation and tracking system. A complete CUI 3.13.6 policy template with video link is appended to this document. The $1795 policy package allows small contractors to prepare an NIST compliant System Security Plan (SSP) in less than 30 hours. This compares favorably to the 110-304 hours estimated by DoD for SSP creation.

The $179/month integrated cybersecurity recurring task management system greatly simplifies documentation and tracking of the hundreds of hours and tens of thousands of dollars of reimbursable recurring tasks needed to comply with FY ’22 DFARS cybersecurity requirements. Effective documentation is key to reimbursement.

The new ACRMS™ templates, free for existing customers, now include individual videos for each policy template. Automatic calculation of the DoD Assessment Methodology or DoDAM scores is now provided. DoDAM scores are required for all new or updated contracts under DFARS 252.204-7012.

ACRMS™ templates incorporate several periodically updated NIST 800 series Special Publications. NIST 800-53 Rev 5 is now fully adopted and there have been quite a few changes which have been incorporated into the new ACRMS™ policy templates. What follows is a detailed list of changes with exact policy numbers and notes for each change. Of the 57 changes, 34 are deemed significant, 3 moderate and 20 minor.

3.1.1, 3.1.2 Significant changes - Adds and removes major parameters to AC-2 and changes some wording for AC-17. We suggest you review the new ACRMS™ template and update your policy.

3.1.4 Significant changes - Revises parameter to identify and document duties of individuals requiring separation. Adds reference to multiple systems and organizations, and that separation of duties policy should span systems and application domains. Adds reference to AC-2 and AC-3 as enforcement mechanisms. We suggest you review the new ACRMS™ template and update your policy.

3.1.5 Significant changes - Adds a parameter to authorize access for individuals or roles. Amplifies a parameter for security functions by deployment in hardware, software,

and firmware. Adds a parameter to specify security-relevant information for which access is authorized. We suggest you review the new ACRMS™ template and update your policy.

3.1.7 Significant changes - Title changed to “Least Privilege | Log Use of Privileged Functions”. Removes specific examples for the control text. Amplifies what privileged functions include and required protections. We suggest you review the new ACRMS™ template and update your policy.

3.1.8 Minor changes - Parameter includes additional selection options when the number of allowed consecutive invalid logon attempts threshold is exceeded. We suggest you review the new ACRMS™ template and possibly update your policy.

3.1.10 Minor changes to parameters. Title changed to “Device Lock”. We suggest you review the new ACRMS™ template and possibly update your policy.

3.1.12 Minor changes in control text. “Remote Access | Monitoring and Control” We suggest you review the new ACRMS™ template and possibly update your policy.

3.1.14 Minor changes in the control text and removes certain parameters. No action necessary.

3.1.15 Minor changes to control text. No action necessary.

3.1.16 Minor changes in the control text. No action necessary.

3.1.18 Minor changes to the control text. No action necessary.

3.1.19 Significant changes - Adds a selection list. We suggest you review the new ACRMS™ template and update your policy.

3.1.20 Significant changes - Added parameter incorporates original text into a selection list. Added parameter defines external systems prohibited from use. Adds privacy policies and plans to the control text. Title changed to “Use of External Systems”. We suggest you review the new ACRMS™ template and update your policy.

3.1.21 Moderate changes - Eliminates parameter selection list and uses 'restricts' in text. Adds parameter value of specific restrictions. Title changed to “Use of External Systems | Portable Storage Devices – Restricted Use” We suggest you review the new ACRMS™ template and update your policy.

3.2.1, 3.2.2 Significant changes - Control text extended to include techniques, updates to literacy training and awareness content, and lessons learned. Adds multiple parameters. Title changed to “Literacy Training and Awareness” We suggest you review the new ACRMS™ template and update your policy.

3.2.3 Minor changes to the control text. Title changed to “Literacy Training and Awareness | Insider Threat” We suggest you review the new ACRMS™ template and possibly update your policy.

3.3.1, 3.3.2 Significant changes - Changes parameter regarding the specific types of events that the system is capable of logging. Requires the review and update the event types selected for logging at a specific frequency. Adds control text regarding inclusion of the potential impact of the inappropriate or unusual activity when reviewing audit records as well as adjusting level or focus of review based on threat or other information. Title changed to “Event Logging” We suggest you review the new ACRMS™ template and update your policy.

3.3.4 Significant changes - Adds parameter text to alert within a specific time period. Title changed to “Response to Audit Logging Process Failures” We suggest you review the new ACRMS™ template and update your policy.

3.3.5 Minor changes to the control text. Title changed to “Audit Record Review, Analysis, and Reporting | Correlate Audit Record Repositories” We suggest you review the new ACRMS™ template and possibly update your policy.

3.3.6 Minor changes to the control text. Title changed to “Audit Record Reduction and Report Generation” We suggest you review the new ACRMS™ template and possibly update your policy.

3.3.8 Significant changes - Adds new alert for specified individuals or roles upon detection of unauthorized access, modification, or deletion of audit information. New parameter supports specifying the individuals or roles to receive alerts. We suggest you review the new ACRMS™ template and update your policy.

3.4.1, 3.4.2 Significant changes - Adds requirement to update baseline configuration document at organizationally-defined frequencies and for organizationally-defined circumstances (in addition to when changes are made). Minor text changes. Changed parameter from specific information system checklists to specific common secure configurations. Adds 'Does not include duplicate accounting of components or components assigned to any other system'. We suggest you review the new ACRMS™ template and update your policy.

3.4.4 Minor changes to the control text. Changed title to “Impact Analyses” We suggest you review the new ACRMS™ template and possibly update your policy.

3.4.6 Significant changes - Adds parameter text for 'mission' essential capabilities. We suggest you review the new ACRMS™ template and update your policy.

3.4.7 Minor changes to the control text and parameters. No action necessary.

3.4.8 Minor changes - Titles changed to CM-7(4) “Least Functionality | Unauthorized Software -- Deny by Exception” CM-7(5) “Least Functionality | Authorized Software -- Allow by Exception”. We suggest you review the new ACRMS™ template and possibly update your policy.

3.5.1, 3.5.2 Significant changes - Removes requirement to change default content of authenticators prior to information system installation. New parameter requires specifying events that require changing or refreshing authenticators. Changes 'security safeguards' to 'controls'. We suggest you review the new ACRMS™ template and update your policy.

3.5.3 Minor changes in the control text. Titles changed to IA-2(1) “Identification and Authentication (Organizational Users) | Multifactor Authentication to Privileged Accounts” and IA-2(2) “Identification and Authentication (Organizational Users) | Multifactor Authentication to Non-Privileged Accounts” We suggest you review the new ACRMS™ template and possibly update your policy.

3.5.4 Significant changes - New parameter adds the selection of (one or more): privileged accounts; non-privileged accounts. Title Changed to IA-2(8) “Identification and Authentication (Organizational Users) | Access to Accounts — Replay Resistant” We suggest you review the new ACRMS™ template and update your policy.

3.5.5 & 3.5.6 Significant changes - Removed control step to disable the identifier and associated parameter. We suggest you review the new ACRMS™ template and update your policy.

3.5.7, 3.5.8, 3.5.9, 3.5.10 Significant rewrite of this enhancement. We suggest you review the new ACRMS™ template and update your policy.

3.6.1, 3.6.2 Significant changes - Changes in control text as well as additions. We suggest you review the new ACRMS™ template and update your policy.

3.7.1, 3.7.2 Significant changes - Adds parameters and changes and additions to the control text. We suggest you review the new ACRMS™ template and update your policy.

3.7.3 Significant changes - Control text adds ‘replacement’; control text expanded in several areas. Adds a parameter for specifying information that must be sanitized from associated media prior to removal. We suggest you review the new ACRMS™ template and update your policy.

3.7.5 Minor changes in the control text. No action necessary.

3.8.1, 3.8.2, 3.8.3 Minor changes in the control text. No action necessary.

3.8.7 Significant changes - New control text prohibits the use of portable storage devices in organizational systems when such devices have no identifiable owner. Parameter text changes from 'security safeguards' to 'controls' We suggest you review the new ACRMS™ template and update your policy.

3.8.9 Significant changes - Parameter added for conducting backups of user-level information contained in specific system components. Removes restrictive control text ‘at storage locations’. Title changed to “System Backup” We suggest you review the new ACRMS™ template and update your policy.

3.9.1, 3.9.2 Significant changes - Control text for notification removed. Parameter for specifying time frame for notification removed We suggest you review the new ACRMS™ template and update your policy.

3.10.1, 3.10.2 Significant changes - Adds parameter for specifying output devices. We suggest you review the new ACRMS™ template and update your policy.

3.10.3, 3.10.4, 3.10.5 Minor changes to text. No action necessary.

3.10.6 Significant changes - Control text requires determining and documenting allowable alternate work sites. New parameter includes specifying alternate work sites. We suggest you review the new ACRMS™ template and update your policy.

3.11.1 Significant changes - Control text adds privacy and a statement about integrating risk assessment results and risk management decisions with system-level risk assessments. Requires development and management of security and privacy risk management strategies. Control text adds privacy. We suggest you review the new ACRMS™ template and update your policy.

3.11.2 & 3.11.3 Significant changes - Control text adds requirement to employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned. Title changes. We suggest you review the new ACRMS™ template and update your policy.

3.12.1, 3.12.2, 3.12.3, 3.12.4 Significant additions and changes to the control text and additions to the parameters. Title changes. We suggest you review the new ACRMS™ template and update your policy.

3.13.1, 3.13.2 Significant changes - Control text changes 'boundary' to 'managed interfaces; adds 'and privacy' in reference to organizational security architecture. Control text adds privacy and system components. New parameter requires specifying applicable systems security and privacy engineering principles. Title changes. We suggest you review the new ACRMS™ template and update your policy.

3.13.3 Moderate changes - Title changed to SC-2 “Separation of System and User Functionality” We suggest you review the new ACRMS™ template and possibly update your policy.

3.13.4 Moderate changes - Title changed to SC-4 “Information In Shared System Resources” We suggest you review the new ACRMS™ template and possibly update your policy.

3.13.5 Minor changes to the control text. No action necessary.

3.13.6 Significant changes - Control text removes parenthetical information. New parameter adds selection of (one or more); at managed interfaces; for specific systems. We suggest you review the attached ACRMS™ template and update your policy.

3.13.7 Significant changes - Control text significantly rewritten. Parameter Adds to specify safeguards. Title changes. We suggest you review the new ACRMS™ template and update your policy.

3.13.8 Significant changes - Removes parameter for specifying alternative physical safeguards. Title changes. We suggest you review the new ACRMS™ template and update your policy.

3.13.11 Adds minor changes to the parameters and control text. No action necessary.

3.13.12 Minor changes to the control text. Title change: SC-15 “Collaborative Computing Devices and Applications” We suggest you review the new ACRMS™ template and possibly update your policy.

3.13.13 Significant changes - Control text replaces requirement to establish usage restrictions and implementation guidance with requirement to authorize, monitor, and control the use of mobile code within the system. We suggest you review the new ACRMS™ template and update your policy.

3.14.1, 3.14.2, 3.14.3 & 3.14.4, 3.14.5 Significant changes - Parameter adds '[Selection (one or more): signature based; non-signature based]'; another parameter adds requirement to send an alert to specified personnel. Parameter selection eliminates option to send an alert to specified personnel and adds option to take specified action. We suggest you review the new ACRMS™ template and update your policy.

3.14.6 & 3.14.7 Significant changes - Control text replaces 'Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion' with 'Analyze detected events and anomalies' and replaces 'Heightens' with 'Adjust'. Parameter added for specifying unusual or unauthorized activities or conditions. Control text requires determining criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic. Title changes. We suggest you review the new ACRMS™ template and update your policy.

CUlcybersecurityCompliance.com

NIST 800-171 CUI Cybersecurity Policy and Procedure Form 3.13.6

https://attendee.gotowebinar.com/recording/1762593421620196103

3.13.6 Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

CMMC SC.3.183 Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).

3.13.6 Self-Assessment Workbook Questions

1. Are all business need exceptions to network communications traffic (inbound/outbound) “deny all” policies documented?
2. Does the system deny network traffic by default and allow network traffic by exception?

<Organization Name> <Date of Current Revision>

NIST 800-53 Safeguard SC-7(5)

SC-7(5) BOUNDARY PROTECTION: DENY BY DEFAULT/ ALLOW BY EXCEPTION

CMMC SC.3.183 Deny network communications traffic by default and allow network communications traffic by exception (i.e. deny all, permit by exception)

Deny network communications traffic by default and allow network communications traffic by exception [*Selection (one or more): at managed interfaces; for* [*Assignment: organization-defined systems*]].

Supplemental Guidance: This control enhancement applies to both inbound and outbound network communications traffic. A deny-all, permit-by-exception network communications traffic policy ensures that only those connections which are essential and approved are allowed.

Suggested Policy Clauses:

1. <Organization Name> shall control traffic at the network perimeter and any key internal boundaries of the system. Design of the monitoring equipment shall be done by the <IT Manager> with the approval of the <Compliance Officer>.
2. Default settings at key perimeter and internal boundaries shall be to deny all traffic and accept only approved traffic.

3. Approved traffic will be determined by the <Compliance Officer> and reviewed <annually>.

Implementation Date: ____<Date of Current Revision>_____

Authorizing Official: ____<Name of Authorizing Official>_____

☐ **Inserting my typed signature on the line below I hereby attest that I am an authorizing official or designated representative of an authorizing official and I approve the above Policy/Procedure on behalf of my organization.**

Typed Signature: ____<Typed Name of Authorizing Official or Designee>_____

NIST 800-171A Assessment of Policy Effectiveness

3.13.6 ASSESSMENT OBJECTIVE Determine if, for an organizational system that processes, stores, or transmits CUI:

3.13.6[a] network communications traffic is denied by default.

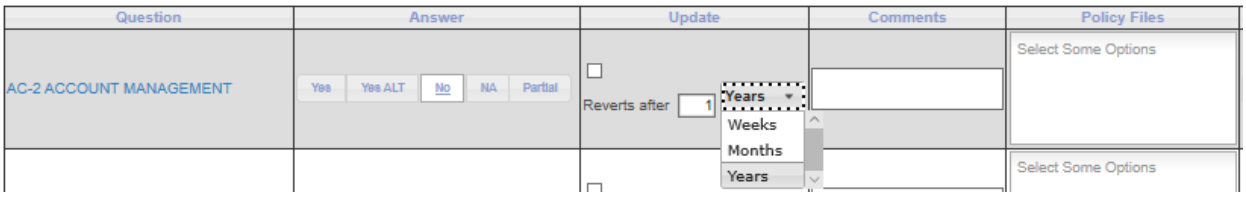
3.13.6[b] network communications traffic is allowed by exception.

CMMC Level 3 Assessment Guide

- Are network communications traffic on relevant system components (e.g., host and network firewalls, routers, gateways) denied by default (e.g., configured with an implicit deny rule that takes effect in the absence of any other matching traffic rules)?
- Are network communications traffic on relevant system components (e.g., host and network firewalls, routers, gateways) allowed by exception (e.g., configured with explicit allow rules that takes effect only when network traffic matches one or more rules)?

Suggested ACRMS data inputs

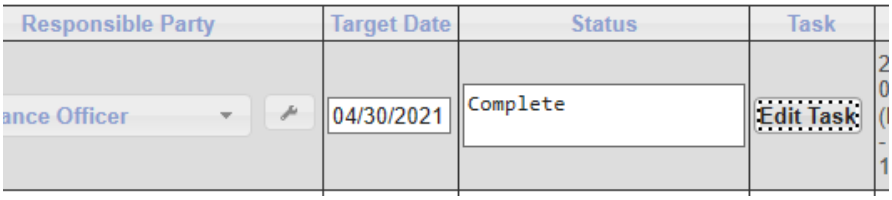
Screen shot of front of ACRMS data input page



Question SC-7(5): BOUNDARY PROTECTION: DENY BY DEFAULT/ ALLOW BY EXCEPTION

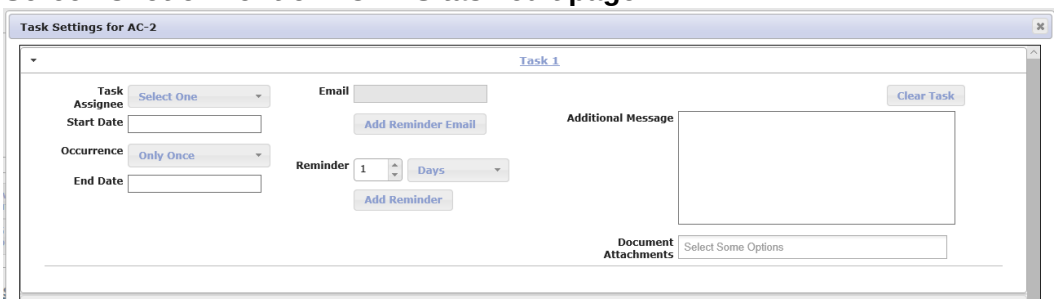
Answer SC-7(5): ☐ Yes ☐ Yes Alt ☐ No ☐ NA ☒ Partial
Update SC-7(5): 1 ☐ Week ☐ Month ☒ Year
Comments SC-7(5): Specify _____
Policy File SC-7(5): CUI 3.13.6 SC7(5) 0221

Screen shot of back of ACRMS data input page



Responsible Party SC-7(5): ☒ Compliance Officer☐ IT Manager ☐ IT Consultant
☐ Other: Specify _____
Status SC-7(5): ☐ Pending ☒ In Process ☐ Complete ☐ Other: Specify _____
Target Date (for task) SC-7(5): ☒ Default (+1 year) ☐ Other: Specify _____
Task Edit SC-7(5): ☐ None ☒ Other: Approved traffic will be determined by the <Compliance Officer> and reviewed <annually>.

Screen shot of front of ACRMS task edit page



Approved traffic will be determined by the <Compliance Officer> and reviewed <annually>.

Hrs/Yr - 2 Staff	Comments - 2 staff	Hrs/Yr - 7 Staff	Comments - 7 staff	Hrs/Yr - 20 Staff	Comments - 20 staff
2.00		2.00		2.00	less if few changes

Estimated hours: 2