Command Cyber Readiness Inspection

Contributing Factors Guide

Version 1, Revision 13
Current as of 16 February 2018

Joint Force Headquarters – Department of Defense Information Network (JFHQ-DODIN)
Chambersburg, Pennsylvania

REVISION RECORD			
Version	**Primary Author**	**Description of Version**	**Date Completed**
V1R2	Rob Diamond	Added Purpose and Process (Sections 1 and 2)	2/1/2013
V1R3	Rob Diamond	Updated sections 1 and 2	2/1/2013
V1R4	Kassy Knouse	Reviewed for standardization, accuracy & completeness.	5/1/2013
V1R7	Ryan Nicholson	Reformatted and updated all references and some wording to reflect Risk Management Framework (RMF) requirements.	5/14/2014
V1R8	Dave Shields	Updated to reflect organizational change from DISA FSO to DoDIN R&SI	9/4/2014
V1R9	Arnold Enfusse	Update ATO, PM, and 8570 requirements	10/27/2014
V1R9	Arnold Enfusse	Updated Command Leadership	12/12/2014
V1R10	Owen Adams	Format and content updates to the entire document	07/06/2015
V1R11	Nick DePatto	Updated Section 3.12, 3.13, 3.14 with new ACAS TASKORD information	04/13/2017
V1R12	John Holliday	Updated references for sections 3.3, 3.5, 3.7, 3.8, 3.9, 3.11, and 3.12	04/25/2017
V1R13	Arnold Enfusse	Format update	02/16/2018

Table of Contents

1. PURPOSE

The Contributing Factors are designed to assist in evaluating the Command's emphasis on compliance of the Information Assurance (IA) Controls that are in place at a site during a Command Cyber Readiness Inspection (CCRI). The inspection items/questions in this document are linked to one or more of the IA Controls as found in NIST SP 800-53. The Contributing Factors evaluates three overall IA areas: Culture, Capability, and Conduct.

Each area must be evaluated and discussed during a CCRI. Once completed the results are then annotated in the nSpect Web Application and become 10% of the final CCRI grade.

2. PROCESS

The Contributing Factors assessment is completed for each network reviewed during a CCRI and results are recorded in the nSpect web application. The results of the contributing factors are provided by interviewing the site Information System Security Manager (ISSM), site security staff, and/or results from technical reviews. There are multiple indicators for each question. If any indicator is "Not Compliant", then the overall rating of the question is "Not Compliant" and indicated as such with a red "X". If all indicators are "Compliant", then the overall rating of the question is "Compliant" and indicated as such with a green "✓". If the question is not applicable, it will be mark with a "NA".

3. PROCEDURES

CONTRIBUTING FACTORS – CULTURE

3.1 Command Leadership Engagement in Cybersecurity Program

Is command leadership (O-7/SES, O-6/GS-15) fully engaged in the Cybersecurity program?

- Command leadership is kept informed of Cybersecurity program status via Cybersecurity/CND updates, IAVM/CTO compliance tracking reports, Stand-up Briefs / Operations Updates, Cybersecurity/CND Dashboards, Internal / External assessments
- Command leadership and AO involvement in CCRI preparation and execution
- Command leadership and AO awareness of the current security state of the networks and enclaves
- Command leadership has awareness of their supporting Intel organization.
- Command leadership receives cyber related Intelligence/Threat Briefings from their supporting Intel organization.

- Command leadership is supportive of IA mission resource requirements and places cyber security as a priority

Reference(s): CJCSI 6510.01F, Enclosure C, 8.C.2, Authorizing Officials.

3.2 Awareness and Implementation of STIG Requirements Requirement

Are administrators aware of and implement STIG/Benchmark requirements?

- Majority of Administrators are aware of and know where to access the STIGs, NSA Guides, and any CC/S/A specific security guidelines (Demonstrated)
- Majority of Administrators reference the above mentioned guides when performing their Cybersecurity responsibilities (Demonstrated)

Reference(s): CNSSI 1253, Appendix E, CM-6; NIST SP 800-53, Appendix F, Security Control: CM-6, CNSSI 1253 - Appendix E – CM-6 – Defined Value for NSS.

3.3 Authority to Operate

Does Site have an Authority to Operate (ATO) for the circuit being inspected and is the ATO current?

- An ATO/IATO signed by the current AO is available
- Has a plan for ensuring that the ATO/IATO and ATC/IATC is renewed prior to expiration of their current approvals
- Site begins working on renewing the ATO at least 90 days prior to the expiration
- Is the site following the Defense Information Systems Network (DISN) Connection Process Guide (CPG)

Reference(s): DoDI 8510.01, Encl 2, para 7f & Encl 6, para 2e(4)(a)&(b); NIST 800-53, Appendix B, pg. B-2; DoDI 8500.01, Encl 3, para 16b; DISN CPG 5.1

3.4 Plan of Action & Milestones (POA&Ms)

Do approved POA&Ms exist for the over 80% of vulnerabilities discovered during the CCRI?

- POA&Ms are feasible and approved by the AO
- POA&Ms include mitigation factors that have been implemented
- POA&Ms are documented and evidence of a tracking method is provided
- POA&Ms include a fix date for when the vulnerability will be remediated

Reference(s): DoDI 8510.01, para 3.i; NIST SP 800-53, Appendix F, Security Controls: CA-5, PM-4.

3.5 Program Managed (PM) System Baselines

Are PM system baselines established and maintained IAW PM Guidance?

- Configuration Management of the PM system baselines is consistent with risks identified and accepted by the AO for the PM System.
- PM Baselines observed adhere to the TFM and patch releases approved by the PM
- Site has contact information for the PM and can access websites distributing information and updates for the PM systems
- Site can demonstrate the process they use to check for updates and have evidence of “keeping in touch” with the PM Office
- ACAS asset lists and results for PM systems are organized and managed to facilitate adherence of the baseline
- Residual risk was documented and considered by the AO prior to allowing the PM system on the network
- Mitigation actions directed or recommended by the PM are in place and enforced
- Critical Concern indicator received on any PM vulnerability scan or technology review during CCRI
- Administrative Access is gained to over 95% of PM system assets

Reference(s): CJCSI 6510.01F Encl C, para 1c.

CONTRIBUTING FACTORS – CAPABILITY

3.6 Computer Cyber Security Service Provider (CSSP) Alignment

Is the site aligned with and leveraging capabilities of CSSP?

- Site is aligned with a certified Tier II CSSP - to be considered “aligned”, site must have both MOA in place and funded.
- A fully executed MOA -OR- the DOD Component has designated the Tier II CSSP that will support the site (documented).
- Roles and responsibilities of the supporting Tier II CSSP and the site (Tier III) subscriber are documented and adhered to.
- Site has contact information and is aware of CSSP support available and complies with reporting requirements (demonstrated).
- Tier II CSSP is integrated into the incident reporting procedures.

Reference(s): DoDI O-8530.2 Encl 3, para E3.3.2.1; CJCSI 6510.01F Encl C para 3.C.(2); DoDI 8510.01, Encl 3, para 3.b; NIST SP 800-53, Appendix F, IR-4.

3.7 External Network Intrusion Detection System (NIDS)-CSSP Monitoring

Has an external NIDS been deployed and is the CSSP monitoring?

- NIDS is located on the wide area network side of the enclave boundary.
- At a minimum the accredited Tier II CSSP should have visibility to all external network traffic.
- If MOA and payment is in place, but no sensors, site must be providing feeds to supporting Tier II CSSP which the Tier II is actively monitoring (must be verified).

Reference(s): NIST SP 800-53, Appendix E, Security Control: SI-4; CJCSI 6510.01F Encl C, para 23a.

3.8 Internal Network Intrusion Detection System (NIDS)-Monitoring

Has an internal NIDS been deployed that is continuously monitored autonomously?

- NIDS has the appropriate architecture to monitor the interior side of the enclave boundary.
- NIDS are under the control of the supporting Tier III organization (enclave level activity) OR there is a formal agreement in place with an accredited Tier II organization to monitor.

Reference(s): NIST SP 800-53, Appendix E, Security Control: SI-4; CJCSI 6510.01F Encl C, para 23b.

3.9 Local Incident Handling

Has a local incident handling program been developed and exercised recently?

- Site has a documented cyber incident response plan.
- Site personnel are aware of the plan and implement it when necessary.
- After action reports, lessons learned, etc., exist showing the plan is exercised, reviewed, and updated as appropriate.

Reference(s): NIST SP 800-53, Appendix F, Security Controls: IR-1-8; DoDI 8510.01, Encl 6, para 1.d; NIST 800-53, IR-9; DoDI 8500.1, Encl 3 para 18g.

3.10 Continuity of Operations Plan (COOP)

Does the site have an executable Continuity of Operations Plan (COOP) that will sustain mission essential functions?

- An alternate site has been designated that will not be affected by the same manmade or natural disaster
- Backup and restoration assets are protected

- Data backup is performed IAW security baseline and NIST SP 800-53, backups are protected and stored off site
- A disaster plan exists that accomplishes restoration/transition of mission essential functions with the time period required IAW control baselines
- Enclave boundary defense security measures at alternate site are equivalent to the primary site
- COOP and disaster recovery plans are exercised IAW with site's control baseline
- Mission essential functions are identified for priority restoration planning
- UPS or backup generators are configured to support key IT assets
- Backups of critical software are available and protected
- Contact list(s) are included and are up-to-date

Reference(s): NIST SP 800-53, Appendix F, Security Controls: CP-1, CP-2, CP-3, CP-4, CP-6, CP-7, CP-8, CP-9, CP-10, CP-11.

CONTRIBUTING FACTORS – CONDUCT

3.11 IA Workforce-DoD 8570 Training

Are administrators adequately trained to conduct IA functions?

- IA Workforce IAM and IAT level designations are consistent with the responsibility levels stated in DoD 8570, and covers military, government civilian, and contractor positions
- Site is at 100% with DoD 8570 Certification compliance requirements. (new employees have 6 months to reach certification)
- Computing environment certifications are maintained that relate to the primary duties of Information Assurance Technical professionals as required by their employing organization.
- IA or IA related training for privileged account holders (non-user level training) (e.g., firewall, incident handling, networking, SRR training, ISSO/ISSM courses)

Reference(s): CJCSI 6510.01F Encl A, para 11b; DoD 8570.1-M para C3.2.4.8.3; DoDI 8500.01, pg 4, para 3.i (1); NIST SP 800-53 Appendix F Security Control: AT-3.

3.12 Configuration Management Processes

Are configuration management (CM) processes implemented and enforced?

- Chartered Configuration Control Board (CCB) (documented) that meets regularly

- Documented standard for configuration (e.g., STIG)
- IA membership in CCB
- Documented CM roles, responsibilities, and procedures to include a change control process that includes IA in review process
- Evidence that the CM process is enforced

Reference(s): CJCSI 6510.01F Encl C, para 19a-b; NIST SP 800-53, Appendix F, CM- 1, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-8, CM-9, CM-10, CM-11

3.13 Comprehensive Vulnerability Management Program

Does the site have a comprehensive vulnerability management program?

- Vulnerability Management Program addresses all vulnerabilities (not just IAVM) that endanger the confidentiality, availability, and integrity of the information and information systems
- System compliance is checked before being placed on the operational network
- System baselines are maintained and updated
- Compliance standards are stated and enforced on all systems whether local owned, PM or rider systems
- There is an effective connection approval process that extends the vulnerability management standard, accountability and reporting to all organizations gaining connectivity through the site's connection to the DoDIN

Reference(s): TASKORD 17-0019 (ACAS); NIST 800-53, Appendix F, SI-2

3.14 Consistent and Repeatable Vulnerability Management Processes

Are vulnerability management processes consistent and repeatable?

- TASKORD 17-0019 compliance
- Rigorous scan – analyze – patch – scan methodology
- Entire IP space is covered by automated scans and patching at least monthly
- ACAS Best Practice Scan Policy is used (if additional policies are specified by USCYBERCOM, they are included too)
- 95+% administrative access on all targets
- All domain and non-domain systems are scanned and patched
- Automated patching capabilities are used for primary OS/Applications and all third party software
- Policy and procedures addressing a removable hard drive environment and deployable/traveling systems are developed and enforced – readiness of these systems is consistent with the garrison network and within acceptable CCRI ranges

- Trend analysis is conducted and shows remediation is effective over time
- No high occurrences of Critical or High vulnerabilities over 30 days old

Reference(s): TASKORD 17-0019 (ACAS); NIST SP 800-53, Appx F, RA-5.

3.15 Identified Vulnerabilities Addressed

Have identified vulnerabilities been addressed immediately?

- Site takes quick fixes for action that have already been approved, but missed on some systems
- Site addresses unapproved/untested fixes via their local CM process, but with a high priority
- Vulnerabilities that cannot be fixed quickly are identified to the ISSO/ISSM/AO and mitigation options presented

Reference(s): NIST SP 800-53, Appendix F, SI-2.

APPENDIX A: ACRONYMS

ACAS	Assured Compliance Assessment Solution
ATC	Authority to Connect
ATO	Authority to Operate
CCB	Configuration Control Board
CCRI	Command Cyber Readiness Inspection
CC/S/A	Combatant Command, Service, and Agency
CM	Configuration Management
CND	Computer Network Defense
CSSP	Computer Cyber Security Service Provider
COOP	Continuity of Operations Plan
CTO	Communications Tasking Order
DAA	Designated Approving Authority
DoD	Department of Defense
DoDIN	DoD Information Networks
DMZ	Demilitarized Zone
IAT	Information Assurance Technical
IATC	Interim Authority to Connect
IATO	Interim Authority to Operate

IAVM Information Assurance Vulnerability Management

IAW In Accordance With

ISSM Information Systems Security Manager

ISSO Information Systems Security Officer

MAC Mission Assurance Category

MOA Memorandum of Agreement

NA Not Applicable

NIDS Network Intrusion Detection System

NIPRNet Non-Classified Internet Protocol Router Network

NSA National Security Agency

PM Program Managed

POA&M Plan of Action and Milestone

R&SI Readiness and Security Inspections

SIPRNet SECRET Internet Protocol Router Network

SRR Security Readiness Review

STIG Security Technical Implementation Guide

TFM Technical Field Manual

TL Team Lead

TLT Team Lead Tool

USCYBERCOM United States Cyber Command