Command Cyber Readiness Inspections (CCRI) Scoring

1D7X1E Training Material

The Overall Classification for this Brief is UNCLASSIFIED//FOR OFFICIAL USE ONLY

Version 1.1 - 23 Mar 2022

What is a CCRI?

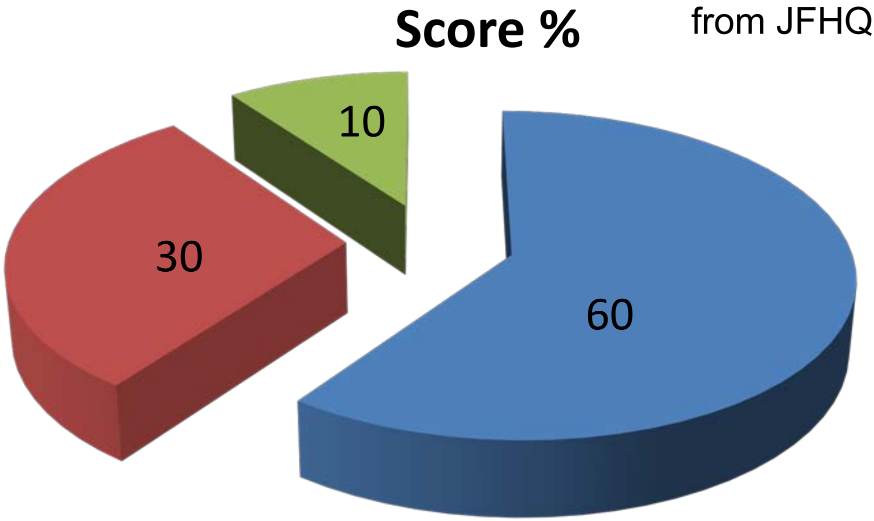
- Command Cyber Readiness Inspections (CCRI) are JFHQ-DoDIN cyber security inspections of the entire base's network.
    - The base/Wing Commander is accountable for the results (and the base Comm Sq Commander is usually responsible for ensuring the base network is secure).
    - *In extreme cases, failing a CCRI could result in shutdown of the base network and disciplinary action for base Comm Sq leadership.*

- CCRIs can be scheduled several months in advance or "no notice" with only a couple weeks notice. The base should continuously security its network.

- CCRIs include three major categories: Technical Areas (60%), CND Directives (30%), and Contributing Factors (10%)
    - For Technical Areas, different parts of network security are scored separately (network infrastructure, vulnerability scans, etc.). Results are combined (and weighted) to create the Technical Areas score

CCRI Components

from JFHQ-DoDIN's CCRI resources



🟦 Technical

- Network Infrastructure
- Domain Name System
- Wireless Technologies
- Host Based Security System (HBSS)
- Traditional Security
- **Network Vulnerability Scan**
- Other Areas:
  Cross Domain Solutions (CDS)
  Releasable Space (REL)
  Web Server
  Database
  Exchange
  Video/Voice Over IP (VVOIP)

🟥 CND Directives

CTO 07-015 PKI Phase II (NIPR Only)
TASKORD 12-0863 SIPRNet PKI (SIPR Only)
TASKORD 17-0019 (Scanning and Remediation
OPORD 16-0080 (HBSS/EPS Deployment)
TASKORD 13-0651 Insider Threat

(Though 1D7X1Es might serve different roles, they are traditionally involved in the "Network Vulnerability Scan" technical area. This includes patching vulnerable computers on the network, or removing/reimaging them to improve the base's scans.)

🟩 Contributing Factors

Culture
Capability
Conduct

How does this affect 1D7X1Es?

- Primarily, 1D7X1Es are involved in *remediating* (i.e. patching) vulnerable computers on the network.
    - Though automated patching systems like Microsoft Endpoint Configuration Manager (MECM, previously known as SCCM) and ARAD should patch most vulnerabilities, they traditionally do not patch 100% of vulnerable systems.
    - 1D7X1Es may have to troubleshoot why some systems are not patching, or may have to wipe/reimage the base's most vulnerable systems.

- The average score for all computers on the network (based on ACAS scans) should be below 2.5 (for a "minor" rating).
    - A single "Critical" or "High" vulnerability on a computer adds 0.67 points to its score ("Medium" and "Low" vulnerabilities add 0.27 and 0.07 points).
    - **An average vulnerability score of 3.5 or higher is considered "Critical" and could contribute to the base failing their CCRI.**

- **1D7X1s are usually the last line of defense for fixing vulnerable computers.**

Concern Indicator(value)		Non-Scanning % Open of Potential
Critical (5)	3.5 or greater	20% or greater
Moderate (3)	2.5 or greater AND less than 3.5	10% or greater AND less than 20%
Minor (1)	Less than 2.5	Less than 10%
Minimal Concern (.5)	Zero CAT Is AND CAT IIs are less than 1.25 AND CAT IIIs are less than 1.25	Zero CAT Is AND CAT IIs are less than 5% AND IIIs are less than 5%
No Concern (0)	0 findings	0 findings

For more information about the CCRI program, please follow this link to JFHQ-DoDIN's site (requires Intelink login):
https://intelshare.intelink.gov/sites/jfhq-dodin/JD/SitePages/CCRI%20Program.aspx