The overall classification of this briefing is:
UNCLASSIFIED

JFHQ-DODIN

STRENGTHEN POSTURE – DRIVE READINESS – DECREASE RISK

AFCEA 2024

Cyber Operational Readiness Assessment

Secure, Operate, and Defend the DODIN

27 June 2024

JFHQ-DODIN Panel

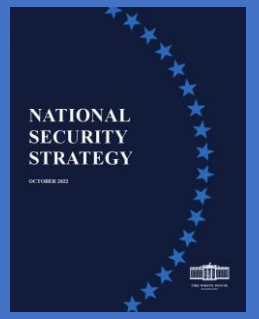
Agenda

- Objective
- Road to Cyber Operational Readiness Assessment (CORA)
- Risk-Based Metrics
- CCRI to CORA Program Differences
- Let's Take It Down a Level
- CORA Components
- CORA High Level Operational View
- Q&A

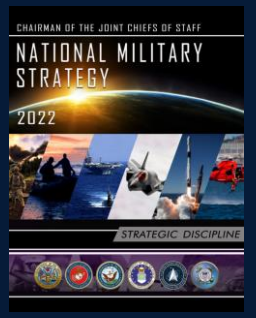
Objective Statement

Automation strategies can revolutionize the measurement and quantification of risk across the battlespace; enabling more efficient and effective cybersecurity operations.

National Strategy



Defense Strategy



- Cyber Resilience
- Strengthen Defense
- Agility
- Ruthless Prioritization based on Priorities and Risk
- Integrate Capabilities
- Partnerships

Panel Members

- John Porter, Director, J10
- Robert “Bob” Landreth, Technical Director, J9
- Stephen Moitoso, Chief Assessment Integration, J10
- Charles Wille, Acting Deputy Director, J10
- Nicholas DePatto, Chief Terrain Assessment Division, J10

The Road to CCRI and Shift to CORA

1. Initiate revamp of CCRI.	2. Strategic Pause to Develop CORA	3. Pilot / Refine / Iterate / Train Teams	4. Kick-off Rebranded CORA

CCRI 1.0 Phase IV — *MAR 2022*

How does JFHQ-DODIN stay flexible in the Cyber Domain in keeping pace with an ever-changing landscape where threats and vulnerabilities are both known and unknown while enabling DODIN Area Operations (DAO) Commanders/Directors to make the right decision when applying resources to increase the security posture of their network.

MAR-JUN 2023

- Overhaul Scoring rubric, incorporate risk-based metrics and Key Indicators of Risk (KIOR)
- Integrate changes into inspection platform, DODIN Inspection Analysis Tool (DIAT) NIPR & SIPR

1st Round Pilots — *JUN - AUG 2023*

- U.S. Naval Academy
- Defense Counter-intelligence and Security Agency
- F35 Lightning II Joint Program Office

2nd Round Pilots — *SEP - DEC 2023*

- 316th Airlift Wing
- Defense Intelligence Agency
- Defense Threat Reduction Agency

Final Pilots — *JAN- FEB 2024*

- High Performance Computing Modernization Program
- 561st Network Operations Squadron
- Air Force Reserve Command

MAR 2024

Strategic Pause → Risk-based Metrics (RBM)

Task: Revise the CCRI to assess the "right things" with metrics that matter. Replace the numerical score and pass/fail with risk.

Harden Information Systems	Reduce Attack Surface	Enable Defense

ACTIONABLE

Weight adjustments reflect RBM priorities; Order, Policies, Directives (ODP) reflect actual results vs Partial, Compliant, Non-Compliant; automated workflow using DODIN Inspection Analysis Tool (DIAT) provides a flexible scoring model designed to iterate and conform to multi-level analysis

CONSEQUENCES

Risk-based exit brief communicates better with senior leaders with **clear** standards

FOCUSED ON RISK

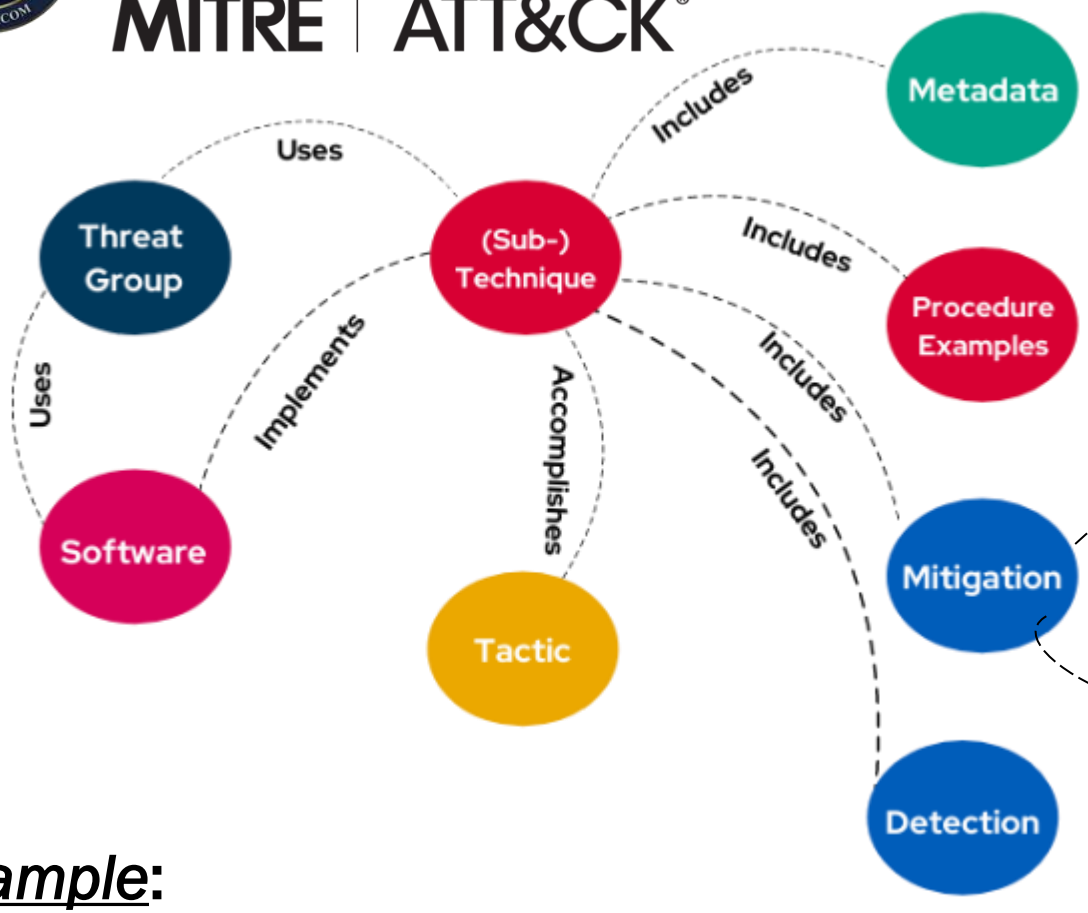
RBM tie directly to CORA scoring through severity and critical overrides (i.e., Key Indicators of Risk) impacting CORA scoring and reinforcing the significance of DCO-IDM priorities established by JFHQ-DODIN

DRIVEN BY PRIORITIES

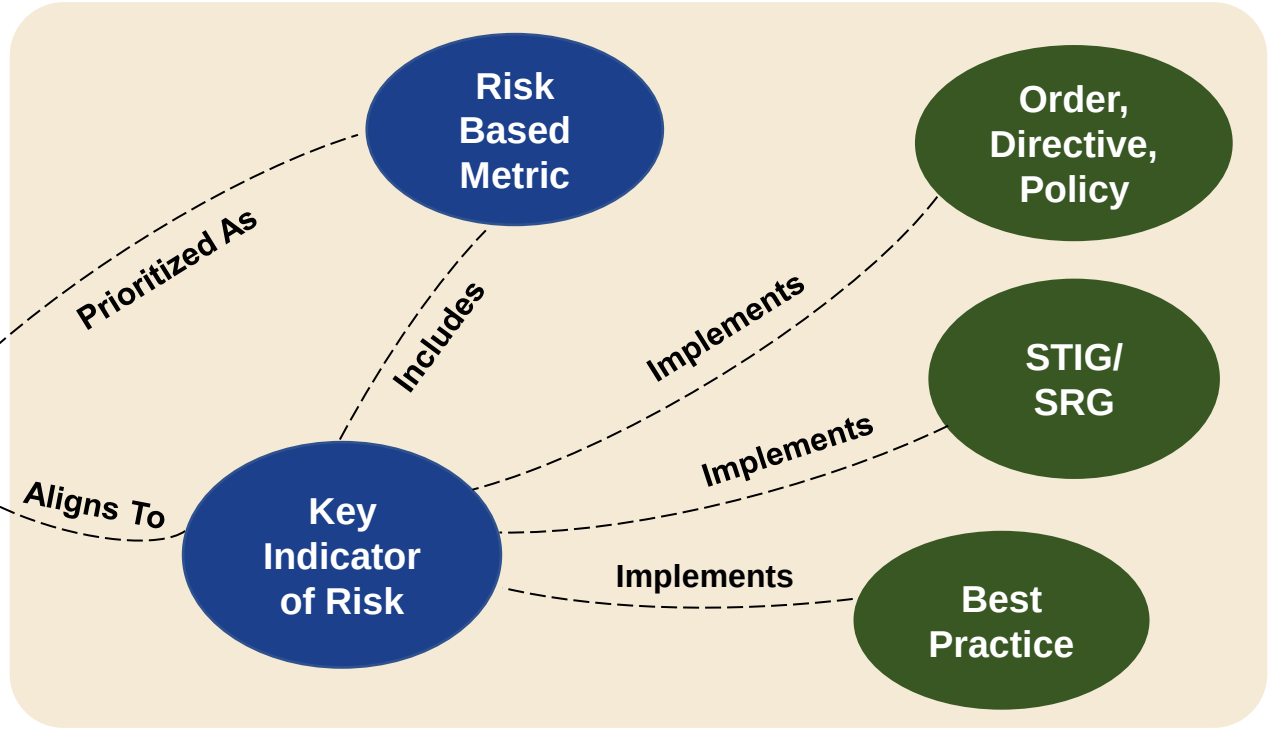
Aligned CORA Criteria with DCO-IDM METs and DAO Roles and Responsibilities; Criteria focus on Control Access, Minimum Defensive Posture, and Detection of Anomalies; Scheduled focused on high-risk terrain

CORA Priorities Mitigate Adversary Risk

MITRE | ATT&CK®



Risk Based Metrics developed from MITRE ATT&CK® and through Key Indicators of Risk directly impact the risk rating for CORA



Example:

Risk Based Metric (RBM)	Key Indicators of Risk (KIOR)	MITRE ATT&CK Mitigations	Mitigation Examples
Encryption Standard	FIPS Encryption (Boundary / Internal)	Mitigates 14 MITRE ATT&CK TTP's	Credential Protection – Network Sniffing; Man in the Middle; etc. Data Protection – Protecting exfiltrated data from being usable

CCRI to CORA Differences and Automation

CCRI PROCESS	Compliance based cybersecurity posture inspection	Largely manual technology reviews and document-based outputs	Sample based manual technology reviews based on STIG / SRG	Pass / Fail an arbitrary line with a post inspection quarantine review board process	High fidelity risk events can't scale nor is timely enough for cyber domain
	Focus	**Workflow**	**Methodology**	**Accountability**	**Future**
CORA PROCESS	Risk-based & threat informed cybersecurity posture inspection	Fully automated workflow and data orchestration / Dashboards / Highly agile & iterative (DODIN Inspection Analysis Tool)	Comprehensive look at boundary / forward facing and focused on the Key indicators of risk	Clear standards and accountability are articulated based on risk	CORA becomes vital data set to "calibrate" and "validate" automated continuous monitoring capabilities

The graphic above is UNCLASSIFIED

Let's Take it Down a Level…

Actual Quantitative Results vs. Qualitative Bands

Orders / Directive / Policies will be actual results 7 out of 9 vs Partial; Compliant; Non-Compliant

Remove Duplicative Checks

CCRI previously had duplicative checks – focus added with KIOR

Risk Focus Changed

Risk indicator (not part of previous CCRI score) removed; modified to reflect Risk Based Metric (RBM) priorities supporting disconnect decisions

Concern Indicators changed to Risk Levels

Critical Concern –> Very High Risk
Moderate Concern –> High Risk
Minor Concern –> Moderate Risk
Minimal Concern –> Low Risk
No Concern –> Very Low Risk

Improve How Results Are Communicated - Not "Pass or Fail"

Executive Summary KIOR sections at the front of report:

- Tech brief (full report with System Administrator (SA's) / SA leadership)
- Key Indicators of risk brief to Commander / Director of organization

Restructure Technology Areas

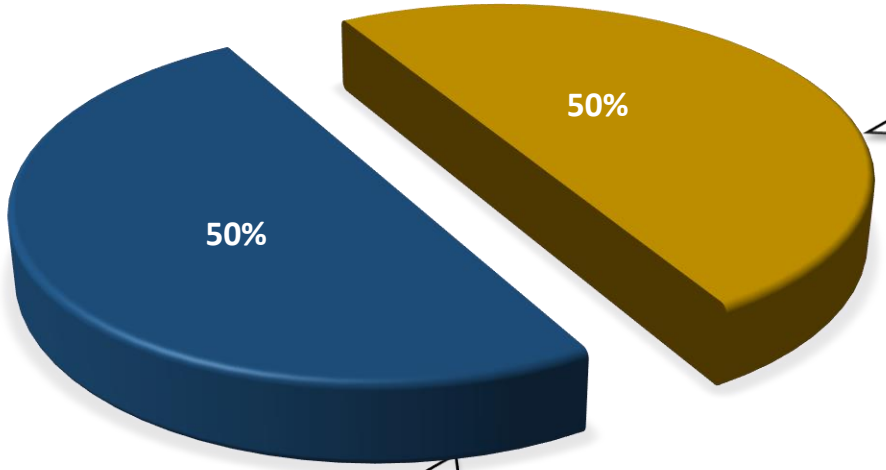
Example: Web would include only Web STIGs and Windows OS would be reflected separately to truly assess individual technology areas

Iterative / Agile Improvement Model

CORA Change Control Board; Voting members; immediate critical updates if necessary; regularly scheduled improvement cycles for changes

- CORA strengthens the posture and resiliency of the DODIN by supporting DAOs in hardening their networks and information systems, reducing the attack surface of their terrain, and enabling defense
- CORA is an agile process encouraging and enabling adjustments in stride
- CORA establishes higher level trust and security of the DODIN as being adaptable to changing threats
- CORA ensures a cyber security foundation is in place using MITRE ATT&CK mitigations, prioritized using threat information, to address adversarial tactics, techniques, and procedures by validating adherence to JFHQ-DODIN Orders and Security Implementation Guides
- CORA is crucial for validating current, future, and emerging technologies that will help the DOD continuously monitor and assess terrain to assess and mitigate risk across the DODIN

CORA Components



Orders / Directives/ Policies

- Endpoint Security
- Network Vulnerability Scan
- Insider Threat
- Cyber Defense Monitoring, Detection, Response
- Cybersecurity and Resiliency
- Supply Chain Risk Management

Cyber Maintenance

- Boundary
- Cross Domain Solution
- Network Vulnerability Scan
- Endpoint Security
- Internal Network
- Domain Name System
- Traditional Security
- Mobility
- Internal Web Server
- Internal Database
- Releasable Networks
- Exchange
- Video/Voice Over IP
- Virtualization/Virtual Infrastructure
- Windows/UNIX OS

Severity Overrides

- Boundary vulnerabilities tied to Key Indicators of Risk result in a severity override of two levels
  - Example: Moderate Risk → High Risk → **Very High Risk**
- Internal vulnerabilities linked to Key Indicators of Risk result in a severity override of one level
  - Example: Moderate Risk → **High Risk**
- Measure indicators linked to Key Indicators of Risk will result in Critical Override
- Mitigation demonstrated may negate a severity override pending Team Lead determination
- KIOR can be remediated / validated during CORA

The graphic above is UNCLASSIFIED

CORA Automation Opportunities

Risk = (Vulnerability – Mitigation) * Impact * Threat

- Continuous Terrain/Mission Mapping – Understanding the infrastructure supporting Mission Critical Terrain and the dependencies
- Terrain Ownership – Automated identification of terrain owners
- Mitigation Analysis – Automatically overlay cyber threat intel to existing infrastructure protections / configurations
- Automated Validation – The ability to provide systematic proof of identified risk areas being mitigated
- Artificial Intelligence – Provide the ability to automatically perform terrain analysis against threat intel
- Cloud posture analysis - Validation to Cloud standards

Vendor engagements please contact JFHQ-DODIN J9 at:

JFHQ-DODIN.MEADE.J9.MBX.J9@MAIL.MIL

CORA High-level Operational View

Prioritized Continuous Assessment of Risk Leading to Operational Effectiveness

Risk-based Metrics

Based on Threat Intelligence & MITRE ATT&CK® Mitigations to *Assess the "Right Things"*

Control Access

Maintain Minimum Defensive Posture

Detect Anomalies

Device Category
- Forward Facing
- Boundary
- Internal

Vulnerability Metrics
- End Of Life Support
- Network Scanning
- Critical Exploitation Vulnerabilities
- Privilege Shell Logging
- Account Management
- Encryption Standards

Mitigation Metrics
- 802.1X Port Security
- End Point Security
- Network Traffic
- Monitoring

Set the Globe

Collaborative data-driven Mission Selection Process to *Assess the "Right Places"*

Secure, Operate, and Defend the DODIN

Assess Terrain

Support DAO commanders & directors in efforts to *Assess for "Mission Success"*

- Key Indicators of Risk
- Technology Reviews
- Directives, Orders, & Policies

CORA provides commanders & directors a more precise understanding of their high-priority cyber terrain & cyber security defensive posture enabling greater C2 & enhancing decision making

Set the Theater

CORA results increase attention to DODIN-related risk factors for combatant commands who have been designated a priority & operations in direct support of that command

Key Outcomes:

- Harden Information Systems
- Reduce Attack Surface
- Enable Defense

Measure Outcomes — *Agile & Iterative Improvement Loop* — Modify Design

JFHQ-DODIN

Postured for Today's Competition & Ready for Tomorrow's Fight