FORWARD®

From ATO Theater to Network Assurance

Automating the "Known" to Defend the Unknown

Sean Deveci

Federal Technical Systems Engineer | Forward

The Problem: Does This Sound Familiar?

6

MONTHS

to gather data for one network ATO

- Manual config pulls from every device
- Spreadsheets that contradicted each other
- Engineers chased for knowledge that lived nowhere else
- By submission time, some data was already stale

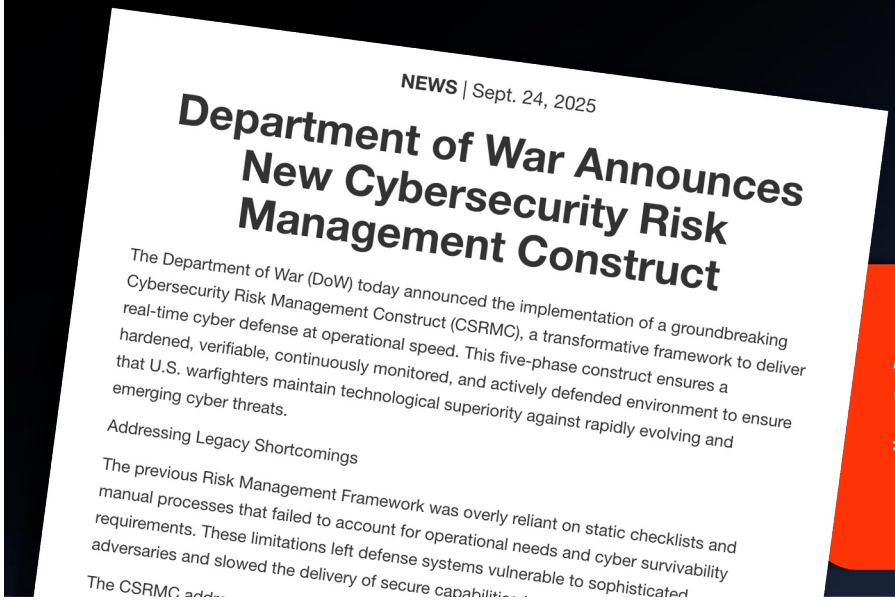
This is not an edge case. It is the standard.

And in September 2025, DoD officially acknowledged it.

FORWARD®

DoD Agreed. RMF Is Being Replaced.

September 24, 2025: DoW announces the Cybersecurity Risk Management Construct (CSRMC)as the direct replacement for the Risk Management Framework.



NEWS | Sept. 24, 2025

Department of War Announces New Cybersecurity Risk Management Construct

The Department of War (DoW) today announced the implementation of a groundbreaking Cybersecurity Risk Management Construct (CSRMC), a transformative framework to deliver real-time cyber defense at operational speed. This five-phase construct ensures a hardened, verifiable, continuously monitored, and actively defended environment to ensure that U.S. warfighters maintain technological superiority against rapidly evolving and emerging cyber threats.

Addressing Legacy Shortcomings

The previous Risk Management Framework was overly reliant on static checklists and manual processes that failed to account for operational needs and cyber survivability requirements. These limitations left defense systems vulnerable to sophisticated adversaries and slowed the delivery of secure capabilities.

The CSRMC addr

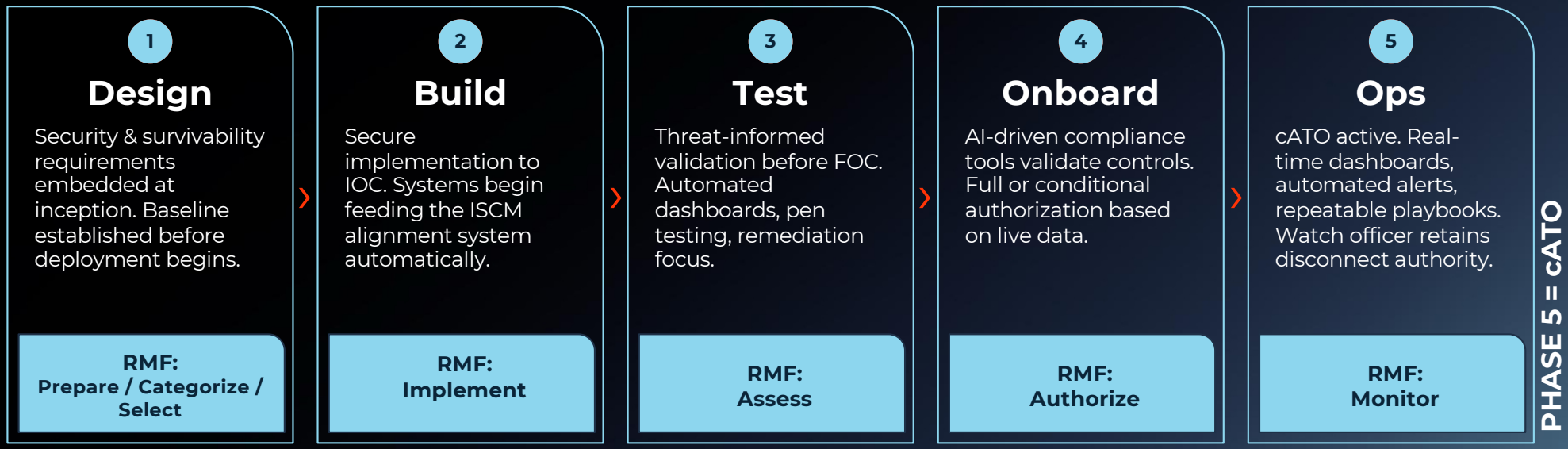
CSRMC Requires

- Continuous monitoring
- Automated data collection
- AI-driven authorization
- Persistent cATO model
- Human oversight at every control point

Overly reliant on static checklists and manual processes that failed to account for operational needs and cyber survivability requirements — leaving defense systems vulnerable to sophisticated adversaries.

— DoD CSRMC Announcement, September 2025

The 5-Phase CSRMC Lifecycle



FORWARD MAPPING

Continuous, vendor-agnostic collection — a live model of what your network actually is.

CSRMC Phases 1 2 4 5

FORWARD NQE

Structured queries against the digital twin. Precise, repeatable answers on demand.

CSRMC Phases 2 3 4 5

FORWARD PATH ANALYSIS

Mathematically verifies behavior matches intent — before and after every change.

CSRMC Phases 3 4 5

FORWARD®

3 Capabilities. 5 Phases. 1 Continuous Assurance Platform.

FORWARD MAPPING
Network Digital Twin

Continuously collects device data across all vendors.

Generates a live, mathematically-accurate model of what your network actually looks like — right now.

CSRMC Phases 1 2 4 5

FORWARD NQE
Network Query Engine

Structured query language for interrogating the digital twin.

Automates continuous data collection for ISCM, CORA, and ATO workflows. Replaces manual data gathering.

CSRMC Phases 2 3 4 5

FORWARD PATH ANALYSIS
Intent vs. Reality

Mathematically verifies network behavior matches design intent.

Validates segmentation, access controls, and routing — without sending test traffic or manually tracing routes.

CSRMC Phases 3 4 5

80% audit time saved
30+ supported vendors



FORWARD

10 Strategic Tenets // 6 for the Network Team



Automation

Reduce human error. Scale efficiency across the DoDIN.



Continuous Monitoring / cATO

Real-time visibility into threats, vulnerabilities, and compliance gaps through persistent monitoring.



Operationalization

Threat detection, compliance, and proactive monitoring — together.



Critical Controls

Adaptive recovery keeps operations running through disruption.



Cyber Survivability

Continuous monitoring, rapid incident response.



Reciprocity

Accept each other's assessments. Cut duplicate compliance work.

FORWARD®

You Can't Defend What You Don't Know You Have

THE REALITY IN MOST FEDERAL ENVIRONMENTS

- Network diagrams **lag operational reality** by months or years
- **Undocumented devices accumulate** between review cycles
- Engineers carry topology **knowledge in their heads** When they rotate out, that knowledge goes with them
- CSRMC Phase 1 **requires a verified baseline** — most programs don't have one

MAPPING

Network Digital Twin

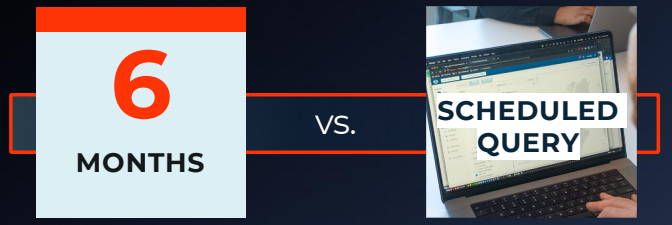
- Continuously collects data from every device, every vendor
- Generates a live, mathematically accurate topology model
- Surfaces undocumented assets automatically
- Reflects network changes in near real-time
- Multi-vendor: Cisco, Juniper, Palo Alto, F5, AWS, Azure + more

FORWARD®

Replacing Manual Scramble with Automated Collection

NQE — Network Query Engine

A structured query language for interrogating the network digital twin. Ask precise, repeatable questions about network state. Get consistent, verifiable answers from continuously updated device data.



ISCM Data Feed

Scheduled queries feed CSRMC Phase 2 ISCM automatically. No manual intervention.

ATO Evidence Package

Same queries, on-demand ATO evidence — current, consistent, audit-ready..

Critical Controls Verification

Pre-built checks verify controls on every in-scope device. Continuously.

Custom Queries

Need custom data? Write your own queries. No vendor lock-in.

FORWARD®

Does Your Network Behave the Way You Think It Does?

EVERY NETWORK HAS TWO 'REALITIES'



What it's supposed to do



What it actually does

The gap between those two layers is where attackers live.

3 **CSRMC Phase 3**

threat-informed validation that controls actually work — not just that they are configured.

FORWARD®

FORWARD PATH ANALYSIS

- **Segmentation Verification**
  Confirms sensitive segments are actually isolated — mathematically verified, not assumed from config review.
- **ACL & Firewall Validation**
  Confirms rules do what they're supposed to — including interactions config review misses.
- **Policy Compliance**
  Continuous checks against network security policy across the full model. Automatically.
- **Change Impact Modeling**
  Model the impact before it hits production. Catch the bad path first.

Authorization with Real Data. Then Keep It Running.

4

Onboard

AI-driven compliance tools validate controls. Full or conditional authorization based on live data.

RMF: Authorize

FORWARD

AI-assisted authorization. Three Forward capabilities converge:

MAPPING	Confirms every device in the boundary is known and documented
NQE	Validates critical controls are correctly implemented across all in-scope devices
PATH ANALYSIS	Verifies network behavior matches the authorization package claims

Result: the DAA authorizes a network they know — not one they hope matches documentation.

5

Ops

cATO active. Real-time dashboards, automated alerts, repeatable playbooks. Watch officer retains disconnect authority.

RMF: Monitor

FORWARD

Forward as the continuous ATO engine:

- Mapping maintains the current network model as the environment changes
- NQE runs scheduled compliance checks — daily, flagging drift as it occurs
- Path Analysis continuously verifies segmentation and access control behavior
- Deviations surface to operators in near real-time
- Watch officer reviews the picture and makes the authorization call

FORWARD > CSRMC Phase Mapping

CSRMC Phase	Requirement	FORWARD Capability	Operational Outcome
1 Design	Verified baseline Cyber survivability requirements	**MAPPING** (Digital Twin)	Establishes accurate network baseline. Surfaces undocumented assets before design decisions are made.
2 Build	Feed ISCM system Implement controls	**NQE** (Auto Collection)	Automates continuous data collection into ISCM. Replaces months of manual gathering with scheduled queries.
3 Test	Threat-informed validation Automated dashboards	**PATH ANALYSIS** (Verification)	Mathematically verifies controls produce intended behavior. Identifies unintended paths before FOC.
4 Onboard	AI-driven authorization Critical controls validation	**ALL THREE** (Converged)	Inventory verified, controls validated, behavior confirmed. Authorization with certainty, not assumption.
5 Ops	Continuous monitoring Watch officer authority	**ALL THREE** (Continuous)	cATO engine in operation. Continuous model, daily compliance checks, real-time segmentation verification.

AI Accelerates the Analysis. Humans Authorize the Action.

Where AI Adds Value

Anomaly Detection
Surfaces deviation patterns manual review would miss.

Predictive Compliance
Flags likely CSRMC gaps before the cATO cycle catches them.

Agentic Workflows
Agents run queries, verify paths, correlate findings — operators get prioritized results.

Why Humans Stay in the Loop

Mission Accountability
Someone owns every authorization decision. Autonomy blurs that chain — policy hasn't caught up.

Adversarial Conditions
Adversaries who learn your automated patterns can manipulate them. Human judgment can't be gamed the same way.

Rules of Engagement
Mission environments often require human sign-off under existing command authority.

CSRMC is not an autonomy mandate. It is a continuous assurance mandate with human decision authority preserved at every critical control point — exactly what the Phase 5 watch officer model requires.

Forward Mapping › NQE Queries › Path Analysis › AI Correlation › **Human Decision**

CSRMC is not a future framework.
It is the direction DoW just gave you.

- The three-year snapshot ATO is being replaced — by policy, not suggestion.
- Every phase of CSRMC has specific network assurance requirements.
- The capability to meet those requirements exists today.
- The barrier is not technology. It is process, culture, and organizational will.

The networks you are responsible for are being probed continuously.
Your assurance posture should match that tempo.

FORWARD®

Q&A

Where is your program in the CSRMC transition?

Still building the Phase 1 & 2 foundation?
Trying to figure out what the cATO actually requires operationally?

Let's talk about what it takes to get there from where you are.

Booth 546

Sean Deveci

Federal Technical Systems Engineer | Forward Networks

forwardnetworks.com/lp/forward-enterprise-federal

DAFITC 2026 | Track 2 | August 24–26, 2026 | Montgomery, AL

2026 Forward Networks Inc.