Security Control Assessor Summit

26 August 2026

Agenda

- Opening remarks
  - Briefer: DAF CISO
- RMF overview and theory
  - Briefer: Dr. Richard Love
- eMASS brief presentation by DISA
  - Briefer: DISA contractors
- Publication updates
  - Briefer: Lt Col Juan Perez & Maj Erik Voron
- RMF Modernization (ServiceNow platform, AO realignment, DevSec Ops ATO balance of speed vs. DoW compliance) & group escalation discussion
  - Briefer: Mr. Kris Johnson & Ms. Nancy Holloway
- 1345-1355: break
- CSSP Alignment & Updates
  - Briefer: Dr. Frieda Clanton
- AO boundary cross-talk discussion
  - Briefer: Mr. Robert Adams
- Closing Remarks
  - Briefer: Mr. Kris Johnson

Opening Remarks

Mr. Robert Bivins:
Acting DAF CISO



Department of War Cyber Risk Management

From Risk Management Framework (RMF) to Cybersecurity Risk Management Construct (CSRMC)

Richard A. Love, JD, LLM, Ph.D.
Professor (Full) National Defense University

UNCLASSIFIED

DoW Risk Management

- RMFs ensure U.S. warfighters maintain technological superiority against rapidly evolving cyber threats. These frameworks dictate how the DoW secures its networks (like the DoDIN), authorizes systems for use, and ensures mission assurance across all operational domains (air, land, sea, space, and cyberspace)
- Without workable and rigorous standards, individual systems will introduce vulnerabilities that compromise military operations.
  - Vital to protect defense networks, secure critical data, and ensure cyber survivability during multi-domain operations.
- September 24, 2025, DoW replaced the legacy Risk Management Framework (RMF) with the Cybersecurity Risk Management Construct (CSRMC) to transition from slow, manual, "snapshot-in-time" compliance checklists to ***dynamic, automated, real-time security***. Department of War.
  - "Department of War Announces New Cybersecurity Risk Management Construct." Official Press Release. September 24, 2025. https://www.war.gov/News/Releases/Release/Article/4314411/department-of-war-announces-new-cybersecurity-risk-management-construct/

CSRMC Goals

- Reduce Bureaucracy: Eliminate the massive paperwork burden that plagued RMF.
- Enable Continuous Authorization to Operate (cATO): Allow systems to stay constantly authorized through live telemetry rather than waiting months for manual reviews.
- Enhance Cyber Survivability: Ensure systems are hardened by design to operate in contested environments against sophisticated adversaries.

UNCLASSIFIED

CSRMC Five-phase lifecycle

Purpose: RM is continuous and aligns with system development and the operational lifecycle.

- **Design:** Security planning / risk tolerance embedded from the outset.
- **Build:** Secure implementation and integration of controls.
- **Test:** Stress tests and validation before operational deployment.
- **Onboard:** Automated continuous monitoring begins when systems are live.
- **Operations:** Real-time monitoring, dashboards, and alerting support ongoing assurance.

UNCLASSIFIED

CSRMC's 10 Foundational Tenets

Shift from static compliance to dynamic, automated, threat-informed defense to ensure cyber survivability during operations.

- Represent a philosophical shift—away from compliance for its own sake, toward mission-aligned, data-driven, and automated risk governance.

1. **Automation:** Leveraging automation to streamline risk management processes, drive efficiency, enhance scale, and reduce human error.
    - Automated evidence collection and compliance activity.
2. **Critical Controls:** Focus on identifying, tracking, and prioritizing the specific security controls that matter most to mission assurance and cyber resilience
    - Not treating all theoretical risks equally.
3. **Continuous Monitoring** (CONMON), Control & ATO: Replacing "snapshot in time" assessments with real-time situational awareness and continuous monitoring to achieve and maintain a ***constant Authority to Operate*** (cATO) posture.
4. **DevSecOps:** Support agile software development by seamlessly integrating security and automation into continuous development, testing, and deployment pipelines (Continuous Integration and Continuous Deployment/Delivery [CI/CD] to safely accelerate capability delivery.
5. **Cyber Survivability:** Ensure systems are designed and hardened to operate, defend, and recover effectively in contested environments against sophisticated adversaries, under attack or partial degradation.

UNCLASSIFIED

CSRMC's 10 Foundational Tenets

6. **Training:** Implement role-based training programs to upskill personnel (operators, engineers, program managers) so they understand dynamic operational cyber risk, evolving challenges, and new automated standards.
7. **Enterprise Services and Inheritance:** Share security controls, proven frameworks, baseline services, and policies across programs to increase adoption, maintain operational consistency, and reduce duplication of compliance burdens.
8. **Operationalization:** Ensure that stakeholders have near real-time visibility into an organization's cybersecurity risk posture to strengthen threat detection, incident response, and proactive monitoring.
9. **Reciprocity:** Allow different commands or components to accept and use other's security assessments and approvals to share information, save system resources, and eliminate duplicative testing.
10. **Cybersecurity Assessments:** Integrating threat-informed testing methodologies (like live penetration testing and threat emulation) with mission-aligned risk management processes to continuously validate a system's security.

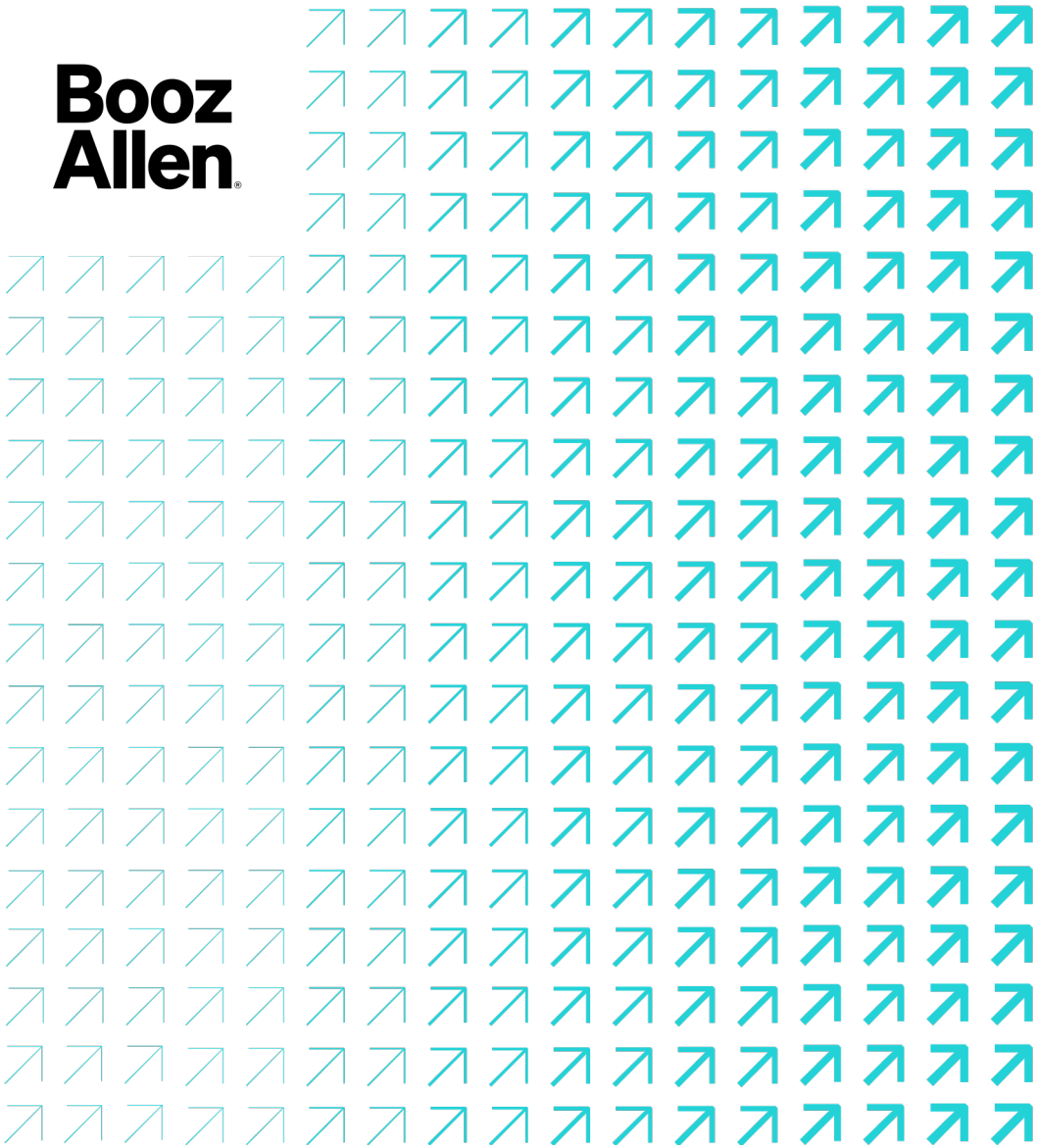
UNCLASSIFIED

Biggest Impact on:

- DoD and military systems: CSRMC's initial scope is the DoD ecosystem—systems connected to the DoD Information Network (DoDIN) and other mission-critical infrastructure. This framework governs how systems are developed, tested, deployed, and monitored across the department.
- Contractors and supply chain partners: CSRMC does not directly replace other programs like Cybersecurity Maturity Model Certification (CMMC), its operational emphasis may influence contract expectations and reporting requirements for defense contractors, especially those who supply software, systems, and operational technology to the DoD.
  - Contractors may soon be expected to provide continuous monitoring evidence, automated telemetry, and integration with DoD security dashboards—an intersection of government risk management and private sector implementation.

UNCLASSIFIED

Booz Allen



AI-Enabled ATO

Navigator.AI for EMASS

- **August 2026**

Distribution: For intended client-only. ROM contains estimate information for budgetary purposes only and can contain Booz Allen proprietary information. In accordance with FAR Part 15.201, contents are provided with the intent to exchange information with the Government, consistent with procurement integrity requirements per FAR 3.104. Content is not intended to be directly incorporated into terms of a future competitive procurement.

boozallen.com

Compliance, RMF, and ATOs

THE CHALLENGE

Challenge 1
System Teams | Creating & Maintaining ATO Packages, SSPs

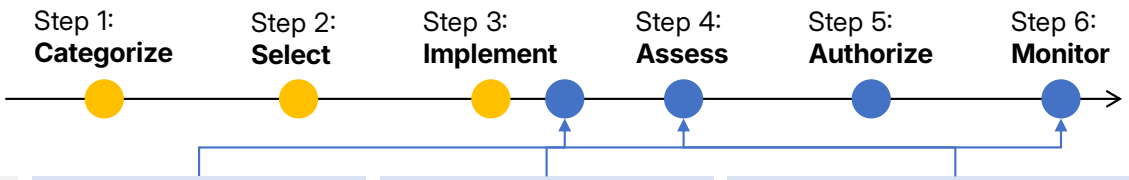
- Create artifacts (e.g., CM Plan) against ~500 Controls, ~3,000 assessment procedures (self-assessment)
- High cycle time on review/feedback from SCAs/validators.
- Difficulty mapping & automating technical data (e.g., scans, live data) to Controls.

Challenge 2
Assessors | Assessing & Monitoring Security Controls

- Too many incoming systems, annual reviews. Varied technology expertise (cloud, on-prem, tactical, etc.).
- Searching across Artifacts (e.g., CM Plan) against ~500 Controls, ~3,000 Assessment Procedures.
- Understanding when system changes over time.

THE SOLUTION

Navigator.AI: Vellox Navigator's Component for AI-Enabled Compliance



Connectors
Collects data from target APIs (e.g., security tools) used for analysis.

Dashboards & Reports
Assessment Agent Controls Report and Summaries for ISSOs, SCAs, and AOs.

Artifact Ingestion and Analysis
Analyzes artifacts (e.g., PDF, Word document, image/architecture diagrams, etc.) using text, vision, and multi-modal models. Maps to Controls.

Retrieval Augmented Generation
Vectorizes artifacts enabling a chat prompt interface with artifacts and information using natural language for ISSOs and SCAs.

Assessment Agent
Autonomous data analysis (artifacts, scan, etc.) against control & assessment procedure security requirements. Recommends control statuses, generates summaries for teams (ISSO/System Owner, SCA/SCA-R/Validator) at both Control & AP (CCI)-level.

Transform DoW System Accreditation with Navigator.AI – Reducing Manual Efforts by Hundreds of Hours per System

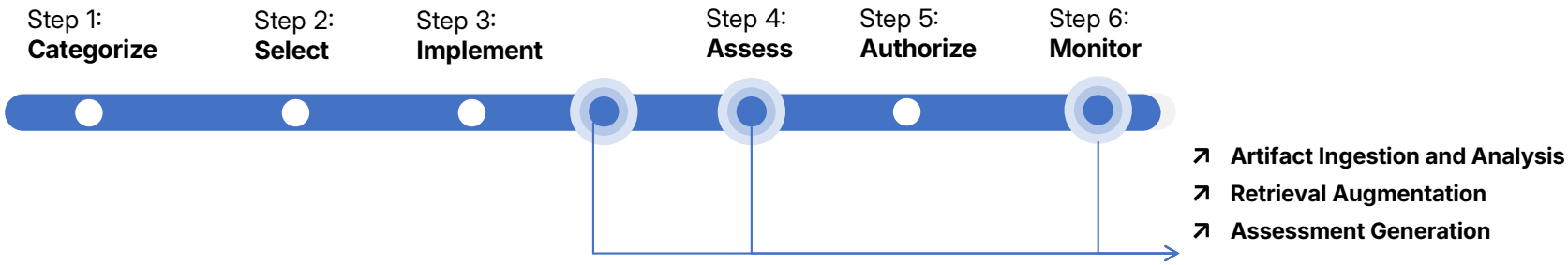
Traditional Accreditation Process: Manual artifact collection and evidence mapping, time-intensive documentation and control validation, extensive review cycles.

Consumes an estimated 1,796 man hours across the ISSO, AO, and Assessor.



RMF Enabled by Navigator.AI: Automate labor-intensive activities, enable teams to improve quality and audit readiness.

Estimated 600 man hours saved per system accreditation, 40% less labor, $90k lower cost per system, and $1.9B in total savings across the EMASS Enterprise



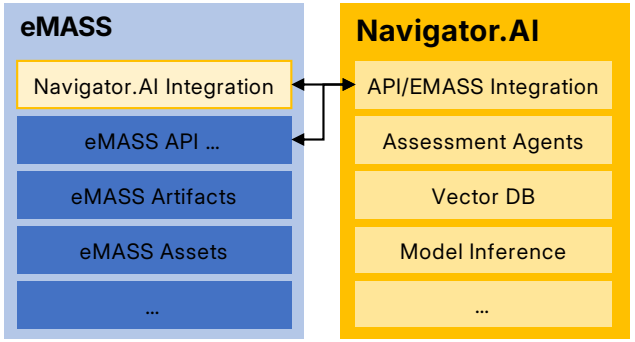
Navigator.AI is Native to EMASS Architecture

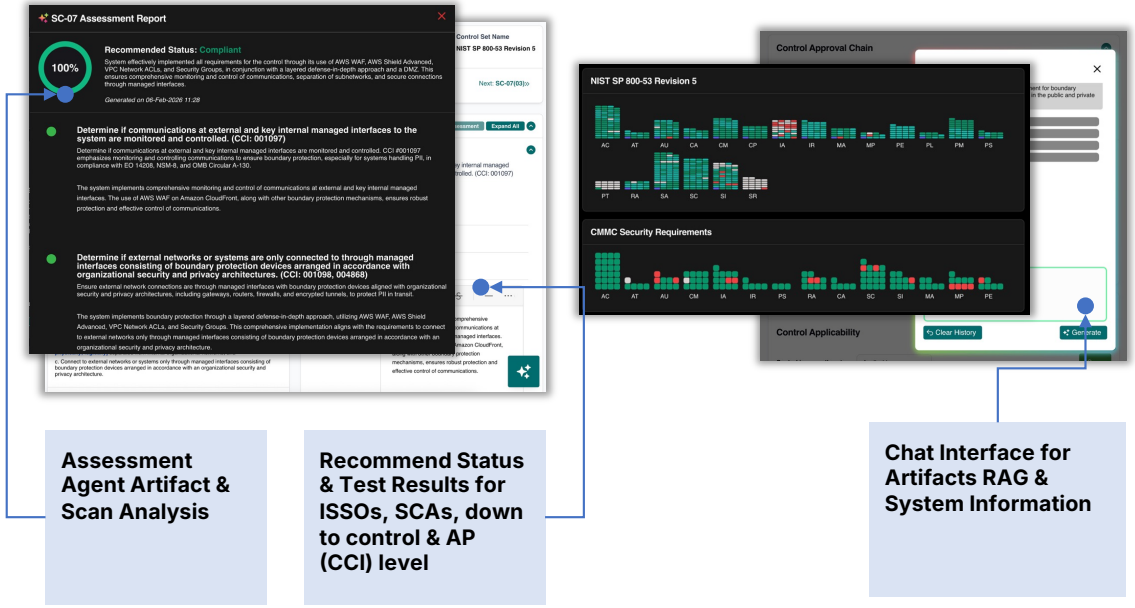
A large amount of compliance processes and systems (i.e., 20K+ ATOs) flow through eMASS.

- Provides AI-enabled functions exposed through eMASS allowing direct support of the DoW ATO process, piloting from different DoW components, teams, various system types, and AOs.
- System Owners currently store artifacts and use eMASS assets & eMASS API for technical/scan data (e.g., STIG results, Container scan results, etc.)

Navigator.AI was designed with DoW and EMASS integration in mind as native features.

- **Native Features:** Functionality is directly provided within existing EMASS instances.
- Users do not have to navigate to other tools/interfaces, upload files to other locations, etc. Navigator.AI is natively integrated with eMASS system artifacts, assets, etc.





BLUF: Navigator.AI is a Strategic First Step Toward Adopting Commercial AI Technology to Advance DISA's Mission

- **In response to DISA's objective to bring commercial AI technology to EMASS, we built Navigator.AI natively on top of EMASS architecture**

Navigator.AI: Agentic workflows that dramatically reduce manual labor required to assess, accredit, and monitor a system

- **Automated Artifact Analysis:** Enable automated ingestion of system authorization artifacts and integration with security tooling
- **AI Powered Control Correlation:** Utilize agentic workflows to automate labor intensive activities required to assess a system, including documentation, evidence collection, and control validation
- **Automated Documentation Generation:** Utilize analysis results to dynamically build content for SSPs, including control implementation statements
- **Native Integration with EMASS:** Built natively on EMASS architecture

Integration Approach

1. Deploy Navigator.AI to existing EMASS solution
2. Enable Navigator.AI for targeted group of pilot DoW organizations that have demonstrated interest in AI driven assessment workflows, allowing organizations to evaluate operational performance and mission impact (e.g., CDAO)
3. Refine and scale Navigator.AI across the Enterprise following pilot validation, incorporating lessons learned, performance insights, and user feedback to drive broader adoption

Intended Outcomes

1. ~1200 man hours saved per system accreditation
2. ~$93,000 in cost savings per system accreditation
3. Time to accredit a DoW system up to 83% faster

Publication Updates

Lt Col Juan Perez & Maj Erik Voron

Publication Updates

- Transition from “sub AO” back to formalized/codified AODR, based in DoDI 8510.01 and AFI 17-101 (Feb 2020 version)

- DoW CISO memo on policy writing
  - Intentional from CNZR to not push out new policies that would likely get rescinded in a couple months due to the new directive

- AFI 17-101
  - Will likely do an interim fix/change based on removing some duplicative language that already exists in higher policy document

RMF Modernization

Mr. Kris Johnson & Ms. Nancy Holloway

RMF Modernization

Topics of discussion:

- ServiceNow platform
- Ongoing system realignments
- Future boundary realignments
- Group escalation discussion
- eMASS training

Break

1345-1355

Please enjoy what's left of the coffee and refreshments

16 AF CSSP (SOC) Strategic Overview

Dr. Elfriede (Frieda) Clanton
Chief, 16 AF/A62 Cybersecurity Governance

August 2026

The overall classification of this briefing is:
CUI

CSSP (SOC) GV and AO Relationship

Per the SAF/CNZ Authorizing Official (AO) Memorandum of Expectations signed by the DAF CISO on March 31, 2025:

*"**AOs** will ensure RMF team aligned every system to a DAF approved Cybersecurity Service Provider (CSSP) IAW reference (d) and (e) **prior to signing ADD and store a copy of the CSSP alignment letter in approved repository**. If you are not using a DAF approved CSSP then a POA&M is needed.*

***AOs** will ensure RMF team has all **CSSP** activities accounted for within a **CSSP alignment letter** for all seven functions below, per references (e), (f), and (g), including but not limited to the seven cybersecurity CSSP functions."*

Key takeaway: The 16 AF GOVERN Team (A6) coordinates with ISSMs, SCAs and AOs across the DAF to enable this process.

(d) DoD Chief Information Security Officer (CISO) Memorandum, Cybersecurity for DOD Networks, 22 Sep 2023
(e) Department of the Air Force (DAF) Chief Information Security Officer (CISO) Memorandum, Change 1, Alignment and Validation of Department of the Air Force (DAF) Information System Owners to designated Cybersecurity Service Provider (CSSP), Oct 2023
(f) DoD Instruction 8530.01, Change 1, Cybersecurity Activities Support to DoD Information Network Operations, 25 Jul 2017
(g) DoD Instruction 8510.01, Risk Management Framework for DoD Systems, 19 Jul 2022

Cybersecurity Activities Crosswalk



Cybersecurity Activities (DoDI 8530.01)	NIST Cybersecurity Framework (CSF) Functions
Vulnerability Assessment and Analysis (VAA)	IDENTIFY, DETECT
Vulnerability Management (VM)	IDENTIFY, PROTECT, DETECT
Malware Protection (MP)	DETECT
Continuous Monitoring (CM)	IDENTIFY, DETECT, RESPOND
Cyber Incident Handling (CIH)	DETECT, RESPOND, RECOVER
User Activity Monitoring for the Insider Threat Program (UAM/IT)	PROTECT, DETECT, RESPOND
Warning Intelligence (WI) and Attack Sensing and Warning (AS&W)	IDENTIFY, DETECT, RESPOND

16 AF CSSP (SOC) Portal

- **SIPR**/**NIPR** portal and repository standardizes ISO submissions to 16 AF CSSP and streamlines system tracking and alignment.
- Adaptive **~200-item** questionnaire tailor's requirements to each ISO's operational environment for alignment accuracy.
- ***System topology, SSP, IRP, HW/SW lists, SLAs*** must be submitted for battle space (cyber terrain) identification.

- **Validation & Cybersecurity Activities**
  - Submitted documentation, combined with ***Security and Incident Response Plan* validation**, confirms responsibility for execution of the seven required cybersecurity activities.
  - Distributed and hybrid environments (SIS I/II, CRG, cloud, hybrid) complicate documentation mapping due to interdependencies and architectural variance that may lead to additional documentation requests.

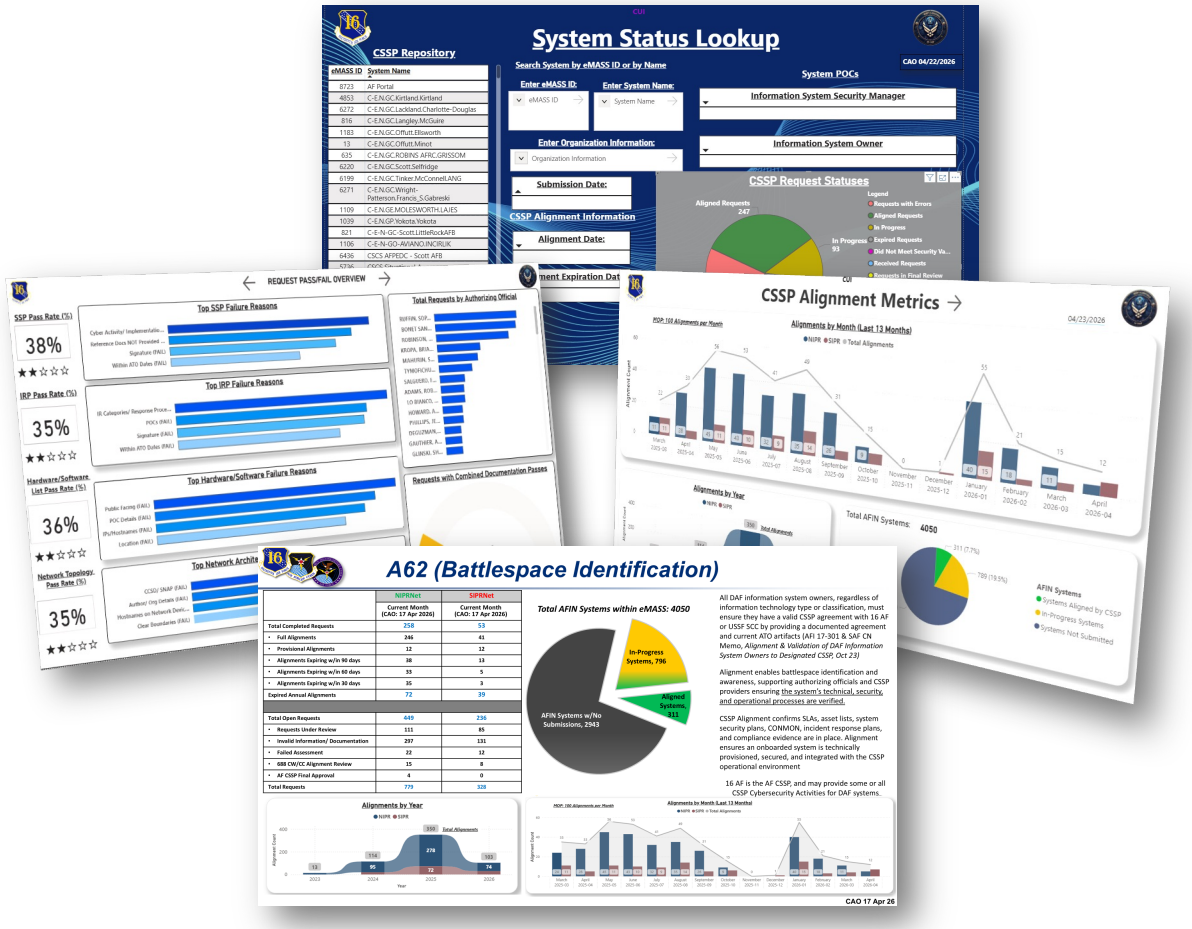
- **Portal's Impact**
  - Standardized interface for ISOs to submit documentation validating security controls, strengthening compliance with ***DoDM 8530.01***.
  - Improved AFIN's battlespace identification and awareness (***OPORD 8600***), supporting DCO.



NOTE: *DCDC inspects the CSSP's alignment process and repository, which includes validating minimum required artifacts.*

16 AF CSSP (SOC) - Reporting & Tracking Dashboards

- Provides a real-time status of CSSP alignments across all AFIN systems.
- Provides Battlespace Identification.
- Fuse data from repositories, artifact reviews, and cybersecurity activity validation into a single authoritative dashboard.
- Identifies non-aligned systems, overdue actions, and external CSSP (C5ISR/DISA/NIWC/HPCMP) services for DCO understanding, reporting and C2.
- Enables senior-leader understanding of the AFIN defensive cyber posture through trend analysis.



Where we are headed……

AI, AI, AI ……

- **Streamline the alignment process**
  - **Remove redundancies with ATO process**
  - **Integration into SOC Dashboards**



We will all go faster…

Objectives: *Align Operations. Integrate Telemetry. Strengthen Governance. Build the Workforce.*

CSSP to SOC Transition

CSSP Model

- *Compliance Driven*
  - Focused on meeting requirements and checklists
- *Perimeter Driven*
  - Relies on network boundaries and static defenses
- *Sensor Focused*
  - Siloed tools with limited context and visibility
- *Reactive Response*
  - Alerts without correlation; slow detection and action
- *Reporting Centric*
  - Point-in-time reporting with limited operational value

SOC Model

- *Capability Driven*
  - Built on mission needs and business outcomes
- *Telemetry Centric*
  - Ingest, correlate, and analyze data across the enterprise
- *Analytics Focused*
  - Context-rich insights powered by automation and AI
- *Proactive Defense*
  - Threat hunting, anomaly detection, and rapid response
- *Outcome Focused*
  - Measurable risk reduction and continuous improvement

What CSSPs Need to Do to Transition

Align Operations. Integrate Telemetry. Strengthen Governance. Build the Workforce.

Operational Alignment

- Map CSSP functions to SOC Levels 1–4
- Define Component roles and responsibilities
- Align incident handling and triage processes
- Adopt SOC maturity and analytics capabilities

Telemetry Integration

- Establish host, identity, application, and network telemetry
- Connect telemetry sources to the Department dashboard
- Validate data quality, coverage, and integrity
- Enable real-time visibility and alerting

Governance Updates

- Update policies, standards, and procedures
- Replace CSSP accreditation with SOC certification
- Align reporting, metrics, and risk management to CISO standards
- Ensure continuous monitoring and compliance

Workforce & Timeline

- Reassign personnel to SOC roles and functions
- Provide training in telemetry, analytics, and threat hunting
- Execute phased transition: **Alignment → Integration → Certification → Retirement**
- Track milestones and communicate progress

SOC Operational Activities, Dependencies, and Outputs by SOC Level

SOC Levels	Key Activities	Key Inputs	Key Outputs
SOC 1 **Monitoring & Data Triage**	• Collect Telemetry • Validate Source Health • Normalize Events • Monitor Alert Queues • Perform Initial Triage • Escalate Validated Activity • Produce DQS Inputs	• Telemetry • Sensor Feeds • Asset Inventory • Configuration • Threat Intel	• Validated Alerts • Telemetry Health • Sensor Status • DQS Metrics
SOC 2 **Incident Response & Detection Engineering**	• Receive Validated Alert • Open Investigation • Enrich with Context • Identify Containment Path • Document Incident • Derive Detection Logic • Produce Response Evidence	• Validated Alerts • Asset Context • Identity Context • Vulnerability Data • Threat Intel • Playbooks	• Incident Record • Investigation Timeline • Detection Updates • Evidence Artifacts
SOC 3 **Threat Hunting & Forensics**	• Develop Hunt Hypothesis • Query Raw Products • Conduct Advanced Analytics • Identify New Detection Logic • Produce Hunt Findings • Recommend Mitigation • Preserve Forensic Evidence	• Incidents • Telemetry Products • Threat Intel • Historic Data • Detection Rules	• Hunt Findings • Campaign Assessment • Forensic Evidence • New Detection Logic • Threat Intelligence
SOC 4 **Mission Defense Command Center**	• Aggregate Enterprise Posture • Monitor DQS & SLSM • Identify Systemic Health • Identify MDEEM Indicators • Identify Systemic Risk • Compile Governance Metrics • Produce Enterprise Picture	• SOC 1–3 Outputs • DQS Metrics • SLSM Scores • Mission Data • Threat Intel	• Enterprise Visibility • MDEEM Scores • SLSM Assessments • Certification Posture • Governance Reports
SOC 5 **AI-Assured Cyber Decision Platform**	• Consume Trusted Analytics • Validate AI Models • Assess Automation Decisions • Evaluate AI Assurance • Produce Audit Artifacts • Execute Approved Actions • Log Audit & Rollback Data	• Enterprise Analytics • AI Models • Playbooks • Threat Intel	• Automation Decisions • AI Recommendations • AI Assurance • Audit Artifacts

Authoritative Sources

As the framework evolves, these sources will guide Department standards, certification requirements, workforce development, AI assurance, architecture decisions, and standard security stacks. Collectively, they provide the foundation for a resilient, interoperable, and continuously improving Cyber Defense Enterprise of SOCs capable of defending Department missions against advanced and AI-enabled threats.

Reference	Role in Framework	Implementation Implication
FISMA	Statutory foundation for agency information security programs.	Supports enterprise cybersecurity governance, accountability, risk management, and agency-wide cyber program oversight.
NIST CSF 2.0	Outcome framework across Govern, Identify, Protect, Detect, Respond, and Recover.	Provides organizing language for SOC outcomes, dashboards, certification, and governance.
NIST SP 800-53 Rev. 5	Security and privacy control catalog.	Supports mapping SOC activities to control families, evidence, and maturity measures.
NIST SP 800-53A	Assessment methods and procedures for examining, interviewing, and testing control implementation.	Used as a professional analogy for certification evidence methods, without making SOC certification a replacement for system authorization.
NIST SP 800-37 Rev. 2	Risk Management Framework guidance.	SOC certification should remain compatible with cybersecurity risk management strategies and continuous monitoring but should not replace authorization.
NIST SP 800-61 Rev. 3	Incident response recommendations and considerations.	Informs SOC 2 response, coordination, communications, recovery, and lessons learned expectations.
NIST SP 800-137	Information security continuous monitoring guidance.	Supports dashboards, continuous evidence, monitoring strategy, and ongoing maturity visibility.
OMB M-26-14	Logging and network visibility driver.	Supports CEM, THIRF, risk-based logging, maturity measurement, retention, and log access concepts.
CNSSI 1015	SOC Certification & Capability Baselines	Establishes minimum SOC standards required to defend National Security Systems (NSS).



AF OCO & CWS
Risk Management Framework

Mr. Rob J Adams
AF OCO & CWS
Authorizing Official Designated Representative (AODR)

This briefing is:
UNCLASSIFIED

As of 13 Aug 2026

Problem Statements

Authorizing Officials are often forced into the "**Nuclear Option**" (denying ATO) or are viewed as operational roadblocks. We lack intermediate levers.

Pretty Paperwork ≠ Security

ATOs are treated as 36-month paperwork drills rather than continuous sustainment.

Root causes:

- Lack of funding
- Training
- Competing priorities

“Stick” Options

Graduated Penalties



Bridge the gap before the nuclear option to enforce system hygiene and accountability.

- Escalations directly to System Owner leadership (GO/SES)
- Imposing harsher, tightly monitored POA&M scrutiny and regular reporting
- Boundary visible score chart for “last scanned dates” & POA&M health

“Carrot” Options

Incentivizing Hygiene

Reward proactive battlespace awareness, continuous monitoring, & genuine security

- Fast-tracking to Continuous ATO (cATO) status
- Granting longer and more flexible ATO lifecycles
- Letters of Appreciation to GO/SES leaders & public shoutouts

Wrap-Up: Embracing the Red

Battlespace Awareness



Owners must know their components, perform routine maintenance, continuously monitor for vulnerabilities, and respond instantly.

A Ready Enterprise



Leadership is **very ready** to shift from point-in-time compliance to risk-based management. Building early partnerships with Mission Owners is critical to success.



Questions

robert.adams.82@us.af.mil

210-977-5082

Closing remarks

Briefer: Mr. Kris Johnson