Mission-focused readiness for DoD

Scalable compliance and automation for cyber operations

CORA requirements

In March 2024, the DoD replaced the Command Cyber Readiness Inspection (CCRI) with CORA. The new assessment focuses on efficient, consistent, and scalable responses to cyber threats. These capabilities require visibility and automation. The main principles of CORA are to harden information systems, reduce the attack surface, and allow a more proactive defense.

Manual processes and visibility gaps limit DoD cyber operational readiness

Confronting rapidly changing cyber threats, U.S. Department of Defense (DoD) cyber operators need comprehensive visibility across the cyber terrain and automated maneuverability to counter new attack vectors. The objective is 24x7x365 operational readiness.

A major barrier to operational readiness is the effort needed to comply with Security Technical Implementation Guides (STIGs) for DoD systems and endpoints. STIGs are released at least once a quarter, and every device can be subject to multiple STIGs identifying up to hundreds of vulnerabilities. Manually assessing, remediating, and documenting compliance for each STIG can take hundreds of hours for senior cyber operators, preventing them from addressing more complex mission activities.

Other barriers to sustainable mission-focused readiness include:

- Limited visibility into cyber terrain.
- Inability to meet continuous compliance demands.
- Lack of interoperability between tools and platforms.
- Prolonged vulnerability exposure windows.
- Resource strain and skill gaps in cyber teams.
- Inconsistent preparation and results for Cyber Operations Readiness Assessment (CORA).

The goal: Cyber readiness with visibility, instrumentation, and automation

DoD cyber defenders can overcome the barriers to 24x7 operational readiness with a joint solution from Red Hat and our partner Agile Defense. The Cyber Operational Readiness—Enterprise solution, 365 C.O.R.E., provides in-depth visibility across the cyber terrain and automates the steps needed for STIG compliance, patch management, incident response, and Enterprise Mission Support Service (eMASS) reporting. The solution combines 2 components:

1. **Red Hat® Ansible® Automation Platform.** Provides a dashboard that operators can use to schedule auditing and remediation activities required for STIG compliance. Ansible Automation Platform executes predefined actions automatically.
2. **DuroSuite®, from Red Hat partner Agile Defense.** Built on Ansible Automation Platform, DuroSuite supplies the platform with the latest STIG audit requirements and remediation actions. DuroSuite automatically produces a record of STIG evaluations and documents each endpoint's security posture as required by Information Assurance (IA) standards and the Defense Information Systems Agency (DISA) Security Requirements Guide (SRG).

How 365 C.O.R.E. meets CORA objectives

Automates STIG ingestion and remediation.

Produces eMASS-ready artifacts.

Provides event-driven playbooks.

Supports infrastructure as code (IaC) and policy as code (PaC) for hardening DoD systems.

Embeds compliance checks throughout the software development lifecycle (SDLC).

Real-world results in the DoD

With 365 C.O.R.E., a DoD agency reduced remediation time for a 24-port switch from 4 hours to 30 minutes, and for a 50-switch environment from 200 hours to 5 hours.

U.S. Army Central (ARCENT) IT Support Services uses DuroSuite to complete tasks in minutes that once required more than 60 man-hours.

Enduring mission value

The 365 C.O.R.E. solution helps the DoD meet DISA CORA goals, including agile, risk-informed assessments, continuous monitoring, and proactive threat mitigation. Mission value includes:

Visibility across the cyber terrain. The 365 C.O.R.E. solution can communicate with any device or operating system that uses Secure Shell (SSH), Session Manager (SSM), or Windows Remote Management (WinRM). The solution monitors the security posture of devices in any location, including air-gapped and cloud environments.

Reduced risk. Automated remediation shortens the time devices remain vulnerable after a new threat is discovered, aligning with the CORA directive to take a proactive stance on cyber defense. Configuration checks, remediation, and generation of artifacts are complete in minutes or hours, compared to days with current processes. Automated remediation also avoids manual configuration errors that can create vulnerabilities.

Increased efficiency for cyber operators. Automating STIG compliance allows less-senior operators to manage the effort, allowing senior team members to focus on more complex projects. Federal agencies using the 365 C.O.R.E. solution report that audit and remediation time decreased by up to 90%.

Scalability across diverse environments. Accessed from a browser, 365 C.O.R.E. avoids the time and costs to procure, deploy, and maintain software agents on each network device.

Achieve sustainable mission readiness by working with trusted DoD partners

The 365 C.O.R.E. solution has demonstrated its value for improving compliance, efficiency, and security posture.

Certifications and compliance validations. DuroSuite received the DoD Authority to Operate (ATO) certification, validating its alignment with DoD standards for STIG automation and eMASS reporting. DISA has published a STIG for Ansible Automation Platform (1 High, 15 Medium, 0 Low severity findings), helping to make deployments more security-focused and scalable. These certifications align with CORA's emphasis on audit readiness and risk reduction in regulated DoD systems.

Increased efficiency and reduced resource strain. DoD agencies using DuroSuite with Ansible Automation Platform report up to 98% reduction in audit and remediation time. The reason is that the 2 technologies work in concert to automate end-to-end workflows from STIG ingestion to artifact generation. Ansible Automation Platform saves more time by providing idempotent[1] Ansible Playbooks for STIG remediation and correcting configuration drift. The playbooks accelerate patching and disaster recovery, both essential for the operational agility required for CORA.

In addition to automating STIG compliance, 365 C.O.R.E. provides:

- Proactive monitoring.
- Adherence to Federal Information Security Modernization Act (FISMA) and the NIST Risk Management Framework (RMF).
- Preparation for CCRI, Command Cyber Operational Readiness Inspection (CCORI), and CORA (see sidebar, "How 365 C.O.R.E. meets CORA objectives").

1 *Red Hat Learning Community blog. "Ansible Idempotence." 26 April 2025.*

Enhanced security posture. Automated STIG ingestion and remediation reduce the attack surface. Continuous monitoring and self healing shorten vulnerability windows. By facilitating 24x7x365 operational readiness, 365 C.O.R.E. helps to foster a collaborative readiness culture that shifts its focus from rigid inspections to operational resilience, zero trust principles, and supply chain security.

Next steps

Red Hat and Agile Defense stand ready to work side by side with DoD teams to swiftly implement 365 C.O.R.E. The typical process involves:

1. **Readiness assessment.** We begin by confirming that devices have the necessary network access, security configuration, and control-node setup.
2. **Hands-on training and baseline auditing.** After a training session, we guide cyber operators through an initial assessment, after which we review audit results and select remediation steps by priority. If needed, we modify Ansible Playbooks to meet specific DoD requirements.
3. **Remediation and optimization.** The solution automatically brings noncompliant devices into alignment with STIG requirements. During this phase, our team guides agency teams to manage compliance deviations and exclusions.
4. **Validation, handover, and support.** Following the initial run, we conduct another audit to measure improvements and validate STIG compliance. For ongoing operations and maintenance, we conduct a rigorous handover process. Teams can also opt for our expert support offerings.

Learn how Red Hat delivers mission-critical solutions and explore more Red Hat resources for DoD teams.

About Agile Defense

Agile Defense stands at the forefront of innovation, delivering advanced capabilities and solutions tailored to critical national security and civilian missions. Whether developing specialized solutions, contextualizing data, or strengthening cybersecurity, our expertise is instrumental in safeguarding our nation's sensitive assets.

About Red Hat

Red Hat helps customers standardize across environments, develop cloud-native applications, and integrate, automate, secure, and manage complex environments with award-winning support, training, and consulting services.

North America
1 888 REDHAT1
www.redhat.com

Europe, Middle East, and Africa
00800 7334 2835
europe@redhat.com

Asia Pacific
+65 6490 4200
apac@redhat.com

Latin America
+54 11 4329 7300
info-latam@redhat.com

facebook.com/redhatinc
@RedHat
linkedin.com/company/red-hat

redhat.com
#2560996_0825