Command Cyber Readiness Inspection

What is a Command Cyber Readiness Inspection (CCRI)? A CCRI is a comprehensive review of a Department of Defense (DoD) entity's cybersecurity posture that includes a detailed assessment of its Information Assurance programs, the non-classified and classified IP networks, and the critical cyber and physical assets that support these networks. CCRI criteria are based on an overall score of 100 percent:

- 60 percent is Technical Implementation – ACAS, HBSS, Network Infrastructure, Traditonal Security
- 30 percent is Compliance with Computer Network Defense (CND) Directives – TASKORDs, OPORDs,
- 10 percent is Contributing Factors such as cyber culture awareness – Culture, Capability and Conduct

Forescout, in implementing Comply to Connect (C2C), will help DoD entities drastically improve their CCRI Score. The C2C framework delivers security through a workflow of phases that include Discover and Classify, Authentication and Authorization, Pre-Connect Compliance and Post-Connect Compliance. Devices connecting to the network are evaluated against pre-configured policies for automated threat detection, incident response, and remediation.

> "The Forescout platform is the core foundation in any C2C framework. Implementing Comply to Connect with Forescout will help DoD entities drastically improve their CCRI Scores."
> **— Niels Jensen, SVP Americas Sales, Forescout Technologies**

Increase your Technical CCRI Component score:

- Gain complete visibility to discover, classify and locate connecting devices agent-lessly; control network access at the access layer—with or without 802.1X authentication; control access based on compliance with security policies; and continuously monitor each device and apply appropriate controls to maintain compliance.
- Increase your CND Directives Component Score: The Forescout eyeExtend Module for Advanced Compliance automates on-connect and continuous endpoint configuration assessment to comply with security benchmarks or STIGs. Deploying this module improves cybersecurity hygiene and regulatory compliance by replacing labor-intensive activity with a process that can be performed automatically and continuously on an enterprise-wide scale.
- Increase several Contributing Factors Component Scores such as Command Leadership Engagement; Awareness and Implementation of Security Technical Implementation Guide Requirements; Plan of Action and Milestones; and Cybersecurity Service Provider Alignment by enabling real-time data sharing at all levels of Command and Control.
- The Forescout platform offers comprehensive capabilities for the DoD's C2C security framework: network-based discovery and classification of all devices, redundant manageability and control of devices, orchestration with mandated security solutions such as Host-Based Security System (HBSS) and Assured Compliance Assessment Solution (ACAS), and continuous monitoring of all connected devices.

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591

Learn more at Forescout.com