



CONR - 1 AF/AFNORTH

Continental United States NORAD Region – First Air Force (Air Forces Northern)
Office of Public Affairs

1210 Beacon Beach Road * Tyndall AFB FL 32403-5549
(850) 283-8080 * FAX (850) 283-3376 * DSN 523-8080

afnorthpa@tyndall.af.mil * www.1af.acc.af.mil * [twitter@1staf](https://twitter.com/1staf) * [Facebook@AmericasAOC](https://www.facebook.com/AmericasAOC)

FOR IMMEDIATE RELEASE

Release 10-05-11/001
May 11, 2010

AFNORTH readies for cyber inspection

By Mary McHale, AFNORTH Public Affairs

TYNDALL AIR FORCE BASE, Fla. – Just as failure is not an option when it comes to 1st Air Force's homeland defense mission, neither is it an option when it comes to the upcoming Command Cyber Readiness Inspection May 17-21.

"This inspection is going to have a lot more teeth than previous ones, along the intensity lines of an Operational Readiness Inspection," said Lt. Col. Dave Wiley, 601st Air and Space Operations Center's Mission Support Division deputy chief. "A critical finding during this inspection could cause the (computer) network to be taken off the global information grid – that's how intense this is going to be."



Previously known as Enhanced Compliance Validations, the newly-named CCRI will be based on past criteria but with two new elements -- contributing factors and more robust grading criteria. Contributing factors are culture, capability and conduct. Culture refers to a comprehensive sense of responsibility and accountability regarding pervasive network issues throughout the organization. Capability refers to the network's sustainability at its optimum level of assigned capabilities. Conduct is simply ensuring the network administration and management processes are correct and enforced.

According to AFNORTH's A-6 Directorate of Communications, the CCRI is a base-level Defense Information Systems Agency Inspection that validates current network accreditations, evaluates enclave and network security, includes network vulnerability scans and assesses compliance with Department of Defense Information Assurance policies.

"Inspectors will be looking at both the secure and non-secure networks, and will grade in three categories: communication areas, contributing factors and traditional security," said Lt. Col. John Ferry, chief, Mission Support Division. "Findings will be classified according to categories and will range from category 1 to category 3. Category 1 represents the most severe threat and must be addressed immediately. Category 2 represents a situation that may threaten and Category 3 represents a vulnerability that impacts mission integrity."

- more -

2-2-2 CCRI

Colonel Ferry added the physical security portion of the inspection will focus on 'traditional security.' This graded area includes properly annotating security documentation, proper safe protocols, shredding documents and escorting uncleared personnel when applicable.

Colonel Wiley said it's the people involved who will ultimately ensure a successful inspection.

"We have a great mix of Airmen and civilians here at 'America's AOC,'" he said. "Our level of experience and expertise is unmatched and based on an especially strong thread of continuity between the military, contractors and civilians. Everyone takes ownership."

Colonel Wiley added he will need that strong thread as the AOC faces unique challenges during this inspection because given their task to execute the homeland defense mission, theirs is not just a computer system -- it's a weapon system.

"Because the AOC equipment is considered a weapon system, it's absolutely critical to ensure all aspects of security are strictly enforced, from installing patches to the cyber system to physical security to proper paperwork documentation."

The Mission Support Division deputy said installing the appropriate patches can be especially challenging because they cannot be 'pushed' automatically; they have to be tested first to ensure they don't compromise the weapon system's integrity. Then, installation must be done individually to each computer that is part of the weapon system.

"For anything we do to our network here, we have to follow guidance given through the weapon system program office at Hanscom AFB in Massachusetts, and each machine's issues must be addressed on an individual basis."

But while daily compliance is the optimum goal, knowledge of what to do in case of a violation is just as important. Information assurance officials said anyone who notices a violation should contact their security manager immediately, who will take care of the matter.

"These issues are not just critical during the inspection -- they are a daily concern to all network users," said Maj. Gen. Garry Dean, AFNORTH commander. "I see all network users working hard to ensure we're all in compliance within our organization and I think everyone realizes they play a critical role to the successful protection and sustainment of our network."