At last, Defense issues wireless rules

04/26/04
By Dawn S. Onley,
GCN Staff

All Defense Department personnel, contractors and even visitors entering Defense facilities must encrypt unclassified information transmitted wirelessly, under DOD's new and long-awaited wireless policy.

The policy, Directive 8100.2, comes nearly two years after DOD issued a policy to oversee wireless transmission of data in the Pentagon. Released this month, it supersedes the Pentagon policy and takes effect immediately. DOD officials had suggested the policy was imminent for nearly three months.

"For data, strong authentication, nonrepudiation and personal identification are required for access to DOD information systems," said Paul Wolfowitz, deputy secretary of Defense. "Identification and authentication measures shall be implemented at both the device and network level."

The policy follows a series of efforts to secure Defense information systems:

- Directive 8500.1, released in October 2002, sets a framework for protecting DOD systems.
- Directive 8500.2, released in February 2003, sets specific standards for securing Defense networks.
- A rule implemented this month requires vendors doing business with DOD to use digital signatures.

The new directive views wireless devices, services and technologies that are integrated with or connected to Defense networks as part of those networks. The policy includes voice and data capabilities that operate as part of the Global Information Grid or as part of a standalone Defense IT system.

GIG is the department's enterprise architecture. DOD sees it as the single global backbone for linking all networks and systems that collect, process, store, disseminate and manage information.

The new policy requires that wireless data encryption be implemented end-to-end over an assured channel and must be validated against Federal Information Processing Standards requirements under the Cryptographic Module Validation Program.

The rule prohibits the use of wireless devices for storing, processing or transmitting classified information without written approval from a designated authority. Classified applications that receive approval must use assured channels with encryption approved by the National Security Agency to transmit data.

Further, cellular, PC, radio frequency and infrared wireless devices are not allowed—without written approval—in areas where classified information is discussed, stored or transmitted. The directive also requires:

- Portable electronic devices that can connect directly to a DOD wired network not be operated wirelessly while connected
- Defense to establish a knowledge management process to promote wireless expertise.

The directive asks organization chiefs to submit implementation plans within 180 days to Defense CIO Francis Harvey detailing how they will comply with the policy.