United States Department of the Interior

FISH AND WILDLIFE SERVICE
Washington, D.C. 20240

DIRECTOR'S ORDER NO. 193

Subject: Fish and Wildlife Service Wireless Implementation

Sec. 1 What is the purpose of this Order? This Order:

a. Provides policy for Fish and Wildlife Service (Service) employees and contractors on the use of desktop and laptop wireless connectivity, and

b. Establishes specific methods of wireless communication to connect to the Service network using Wireless Local Area Networks (WLANs), insecure public Internet Hot Spots, and all cellular based wireless connections.

Sec. 2 What is the scope of this Order? This Order applies to:

a. Service employees and contractors in travel status who may use wireless connectivity to conduct official business in areas such as, but not limited to, Internet Cafés, restaurants, and airports; and

b. Service teleworkers, field employees, and contractors who may operate in remote locations and need wireless access to conduct business operations.

Sec. 3 Does this Order supersede or amend other directives? This Order clarifies the conditions under which the Service authorizes wireless access to address risks defined in the Department of the Interior's Information Technology (IT) Security Policy Handbook.

Sec. 4 What does the Department's IT Security Policy Handbook require and what risks does it address?

a. The Department's IT Security Policy Handbook outlines the security requirements for wireless networking devices. The requirements apply to all devices transmitting Departmental data or interfacing with the Department's network infrastructure, including:

1) Major applications,
2) General support systems, and
3) Any Departmental IT resource using 802.11 standards.

b. Employees must be careful when using Departmental resources to protect them from loss or corruption. The loss of a laptop or Personal Digital Assistant (PDA), while a concern, is less troubling than the loss of sensitive data or information on the laptop or PDA. The risks associated with using wireless technologies are:

1) When connecting to non-Departmental networks or resources, Sensitive But Unclassified (SBU) unencrypted data/information could be inadvertently or intentionally stored or copied to a non-Departmental resource.
2) In places such as airports, hotels, libraries, and cafes/restaurants, laptops, PDAs, and cellular phones connected to any publicly or personally-owned kiosk, computer, etc. are subject to interception.

c. The Departmental guidance recognizes the risks but delegated the authority for implementing wireless and accepting the risks to bureau Chief Information Officers.

Sec. 5 What do Service employees and contractors have to do to use wireless? To reduce or mitigate risk, Service employees and contractors may use wireless for official business only when they meet the following conditions:

a. Users must not rely on wireless availability exclusively for the protection of life and property.

b. Service employees and contractors must follow their Regional and Program procedures to accomplish the following:

1) Provide their computer equipment to Regional or program technical support so that they can follow the Service Security Technical Implementation Guides (STIGs) to secure the laptop operating system configuration. The STIGs and the Regional technical support staff ensure the following:

(a) Users work only on Government-furnished equipment,
(b) The computer's data at rest is encrypted, and
(c) The computer meets Service configuration guidelines for wireless communications.

2) Accept the Service User's Rules of Behavior, which includes wireless access requirements.
3) Read the Service Wireless Threat Training Briefing. This briefing:

(a) Informs users of several types of wireless threats;
(b) Provides steps to combat these threats and avoid common mistakes; and

(c) Includes references and links to current security policies, rules of behavior, and Service Configuration Procedures and Guides.

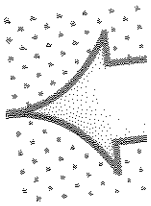
4) Use the FWS 802.11x and broadband STIGs. The objectives of the wireless STIGs are to:

(a) Protect the confidentiality and integrity of data during transmission,
(b) Protect the mobile computing device from security threats, and
(c) Audit security-related events to detect and identify actual and attempted security violations.

c. Instructions for implementing this Order are on the Service intranet.

d. Users who disable, deinstall, or tamper with the security settings or software once configured for wireless use by Regional or Program IT support personnel could have their wireless privilege revoked and face disciplinary action.

Sec. 6 When is this Order effective? This Order is effective immediately. Unless it is amended or revoked, it remains in effect for 18 months after the date it is signed or until we incorporate it into 270 FW 7 of the Fish and Wildlife Service Manual.



Kenneth Stansell

Deputy
DIRECTOR

Date: 2-28-08