Farm Credit Administration

1501 Farm Credit Drive
McLean, Virginia 22102-5090
(703) 883-4000

INFORMATIONAL MEMORANDUM

September 7, 2000

To: The Chief Executive Officer
All Farm Credit System Institutions

From: Roland E. Smith, Director
Office of Examination

Subject: Network Security – Support Web Sites

Electronic networks and the Internet offer Farm Credit System (FCS) institutions the potential for greater operating efficiency and business opportunities. However, the use of this technology also exposes the institution to potential risk. Not only does the use of the Internet as a delivery channel increase the risk of unauthorized access to data; it also poses the threat of an institution's computer resources being used for unauthorized, or illegal activities.

While our examinations have found that FCS institutions have implemented the necessary controls to secure their network systems, effective security protection is a dynamic and continuing process. Computer hackers and intruders continue to exploit newly discovered holes in firewalls and network operating systems and devise new computer virus attacks. In order to protect the confidentiality, availability, and integrity of their data and systems, network administrators must constantly monitor new exploits and ensure that measures to protect against them are applied to their systems.

One of the best ways to monitor for new threats and implement timely corrective measures is to regularly review the advisories and recommended solutions provided by independent or non-profit organizations. There are a number of such organizations and the following three are provided for your reference because they contain an extensive catalog of threats, timely advisories, and links to other related sites.

1. National Institute of Standards and Technology (NIST) – The Computer Security Division at NIST's Information Technology Laboratory (ITL) has created a searchable index containing 700 of the most important publicly known computer security vulnerabilities. The database, called ICAT (not an acronym), provides very specific detail and links users to information at Carnegie Mellon University and Federal response centers. The ICAT can be accessed through the Internet at *http://csrc.nist.gov/icat*. ITL bulletins, including one describing ICAT (July 2000), can be found at *http://www.itl.nist.gov*.

2. System Administration, Networking, and Security (SANS) Institute – This is a cooperative research and education organization through which more than 96,000 system administrators, security professionals, and network administrators share lessons learned and solutions to security problems. One of its products is system and security alerts and news updates. New and re-emergent attacks are recorded, analyzed, and reported through its Global Incident Analysis Center. The SANS Institute Web site is *http://www.sans.org*.

3. ICSA.net (not an acronym) – This organization sets standards, performs research, tracks and measures risks, and certifies 98 percent of the market's anti-virus software, network firewalls, intrusion detection, cryptography and related products. ICSA.net was established in 1989 as an independent corporation to promote the improvement and deployment of security technology. Its Web site address is *http://www.icsa.net*.

The listing of the three sites above should not be construed as a Farm Credit Administration endorsement. However, periodically scanning the above and similar sites may assist network administrators guard against new attacks.

If you have any questions about this document, please call Thomas Glenn, Special Examination and Supervision Division, Office of Examination, at (703) 883-4412, or write to him on the Internet at e-mail address *glennt@fca.gov*.