Farm Credit Administration

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

INFORMATIONAL MEMORANDUM

August 30, 1999

To: The Chief Executive Officer
All Farm Credit System Institutions

From: Roland E. Smith, Director /s/
Office of Examination

Subject: Threats to Information Management Systems

The purpose of this memorandum is to heighten your awareness of the increasing threat to financial institutions, including Farm Credit System (FCS) institutions, from "cyber-terrorism." Cyber-terrorism is generally defined as the use of computing resources against persons or property to intimidate or coerce a government, an entity such as a FCS institution, or persons to disrupt, deny, corrupt, or destroy computer systems or networks. Cyber-terrorists can be individuals, criminal organizations, dissident groups or factions, or another country. Attacks can be generated internally or externally, and may be directly against a computer system, or focus on the supporting infrastructure (telecommunications, electricity, etc.). Cyber-terrorism includes acts of commercial espionage and employee sabotage and can be one catastrophic attack on your infrastructure, or a series of coordinated, seemingly independent attacks. Furthermore, cyber-terrorism does not have to be for the purpose of monetary gain or to obtain information; oftentimes, it is conducted solely to destroy all or part of an information management system.

As we have learned from addressing the Year 2000 problem, the infrastructures are much more interdependent than in the past. Debilitation or destruction of one computer system could have adverse effects on others causing widespread denial of service and other losses.

Financial institutions' vulnerabilities are increasing steadily, and the means to exploit those weaknesses are readily available. Cyber-terrorist attacks can take the form of:

- Denial or disruptions of computer, cable, satellite, or telecommunications services.
- Monitoring of computer, cable, satellite, or telecommunications systems.
- Disclosure of proprietary, private, or classified information stored within or communicated through computer, cable, and satellite or telecommunications systems.
- Modification or destruction of computer programming codes, computer network databases, stored information, or computer capabilities.

♦ Manipulation of computer, cable, satellite, or telecommunications services resulting in fraud, financial loss or other federal criminal violation.

The ultimate threat to computer security remains the insider. Thus, security clearance checks should be required. Common examples of computer-related employee sabotage include:

♦ Entering data incorrectly
♦ Changing data
♦ Deleting data
♦ Destroying data or programs
♦ "Crashing" systems
♦ Destroying hardware or facilities

The major types of threats to financial institutions include the use of computer viruses, “network worms” and “Trojan horses.” Network worms are programs that scan systems or entire networks for available, unused space in which to run. Worms tend to tie up all computing resources in a system or on a network and effectively shut it down. Trojan horses are programs that appear to perform a useful function and sometimes do so quite well but also contain a feature that is usually malicious in nature.

The Internet is a source for numerous varieties of hacker software, some of which are issued in the guise of network administrator tools, freely available for downloading. Some of these "tools" can be secretly attached to innocent-sounding files and, upon execution, embed themselves in a computer system. These innocent programs can be games, utilities, applications, etc. Although some of these tools have legitimate purposes, people with malicious intent can also use these programs for their own goals.

FCS institutions need to address the growing threat of cyber-terrorism when developing and testing disaster recovery/contingency plans. To date, the FCS has encountered few problems. However, because it has become easier to create a cyber attack, FCS institutions are more likely to experience attacks in the future. Having appropriate controls in place and employing some or all of the following procedures and practices may help limit your institution’s vulnerability to attacks.

♦ Maintaining adequate expertise to administer, secure, and monitor network security.
♦ Planning network design and architecture in terms of connectivity, placement of key components, and firewalls, i.e., systems or combinations of hardware and software solutions that enforce a boundary between two or more networks, for technological advancements.
♦ Implementing a physical security program that controls and limits the access to computing and information resources to only those who absolutely require such access.
♦ Incorporating logical access controls to computing and information resources that include a program for issuing user IDs, password requirements, anti-virus programs, and monitoring.
♦ Using a log-in banner to ensure that unauthorized users are warned that they may be subject to monitoring.
♦ Ensuring regular use of virus detection software. Identifying and implementing controls over dial-in modems that gain access to internal networks.

♦ Using secure firewalls and ensuring a process is in place to periodically update firewalls, i.e., systems or combinations of hardware and software solutions that enforce a boundary between two or more networks.

♦ Establishing and enforcing clear security policies for employees.

♦ Educating employees and establishing an environment that leads to enforcement of internal policies.

Ultimately, the best defense against most cyber attacks is having controls in place that call for regular monitoring of network activity, a well-configured firewall, and regular reminders of the institution’s security policies. Further, because rapid technology advances are likely to continue in the future, board and management should expect these controls to be reviewed and updated frequently.

If you have any questions regarding this memorandum, please call Thomas M. Glenn at (703) 883-4412, or correspond on the Internet at e-mail address *glennt@fca.gov*.