Federal Deposit Insurance Corporation
550 17th Street NW, Washington, DC 20429

November 19, 1999

Information Security Precautions

During the Century Rollover Period

To: The Board of Directors and Chief Executive Officers of all federally supervised financial institutions, service providers, software vendors, federal branches and agencies, senior management of each FFIEC agency, and all examining personnel.

Introduction

The Federal Financial Institutions Examination Council (FFIEC) believes that financial institutions may be exposed to higher levels of fraudulent and malicious attempts to exploit information systems during the century date change. Hackers and developers of malicious software may step up their activities at a time when it may be difficult, without adequate safeguards, to detect or distinguish among a routine software or operations problem, a Year 2000-related problem, and fraudulent or malicious activity.

Much of the guidance contained in this statement has been included in various parts of several previously issued FFIEC advisories. This statement is meant to compile that information for ease of reference and to encourage the industry to focus attention on information security as the century date change rapidly approaches. The FFIEC strongly encourages financial institutions to review their security procedures, consistent with the institution's size, reliance on automated systems and risk profile, and where necessary, enhance internal controls and security procedures to deter and detect unauthorized intrusions in late 1999 and early 2000.

Effective Information Security and Steps to be Considered

An effective information security framework is key to maintaining the confidentiality, integrity and availability of information resources. Major components of a framework include information security policies, authentication methods and access controls. Financial institutions should review their information security framework in light of the potential for fraudulent or malicious activity during the rollover period. Financial institutions should consider the following:

- *Staff Awareness* - Brief staff about the need for heightened information security precautions during the rollover period and how they should protect the institution and its customers.

- *Passwords* - Remind staff of the importance of keeping passwords and account names confidential, despite pressures to reveal them by unauthorized parties under the guise of needing them to solve an urgent problem.

  Remind staff to regularly change their passwords. Unless passwords are replaced by smartcards or biometric devices (e.g, fingerprint screening), authorized users should choose passwords that are difficult to compromise. Strong passwords (e.g., passwords that employ unusual combinations of upper

and lower case letters and numbers) that have to be changed on a regular basis form the first line of defense in protecting information resources from unauthorized access.

- *Background Checks* - Ensure that information technology staff, contractors and others that can make changes to information systems have passed background checks. Periodically revalidate logon IDs and access lists.

  Consider limiting access to the data center to key personnel during the rollover period. Similar access safeguards should be considered for telecommunications equipment and key workstations that may provide access to critical systems.

- *Authorize staff to take action* - Ensure that staff on duty has the authority to take defensive actions to protect information systems that become targets of malicious activity.

- *Response Team Information* - Update information on how to contact software vendors, computer emergency response teams (CERTs) and similar information security organizations.

  Ensure that security and system administrators have readily available information on vendor contact points, help desk numbers, special web sites and operating procedures for the rollover period. Establish alert and escalation procedures with clearly defined lines of responsibility to respond to suspicious activity. Ensure that necessary resources will be available when needed to respond quickly to suspicious activity.

- *Contingency Plans* - Review and update, as necessary, the procedures for recovering information systems that may be damaged by malicious activity during the rollover period.

  Business continuity and contingency plans are an important part of a financial institution's information security framework. Such plans define how an institution will recover its critical business processes in the event of a security-related disruption to its operations. Financial institutions should maintain backup copies of data files, books and records stored in electronic form. These backup records will help to ensure continuity of service in the event an organization's information security safeguards are compromised and original data is unavailable.

- *Limit Security Exceptions* - Review procedures and approval levels needed to grant exceptions to security procedures and controls during the rollover period. If Year 2000 or other problems do occur, institutions should ensure they do not compromise important security controls in a rush to fix information systems.

- *Limit Changes* - Limit software and hardware changes to those that are critical to maintain operations.

  If a change must be implemented, ensure that thorough change control procedures are applied and that testing can be completed before the rollover period. Financial institutions should consider using integrity checking software to

identify unauthorized changes that have been made to web sites and other systems.

- *Monitor systems* - Survey your systems configurations periodically to ensure that security controls are in place and operating effectively.

  Ensure that known system vulnerabilities are eliminated or controlled, including those that become known shortly before the rollover period. Systematic vulnerability analysis is an effective way to identify and repair weaknesses in security controls. Establishing partnerships with security experts at peer firms that use comparable information security products is one way to maintain an awareness of system vulnerabilities and share security resources.

- *Review access to systems* - Ensure that there is a timely review of machine logs prior to and during the rollover period, particularly logs of firewalls and remote access service and computer links. These logs should be analyzed frequently for signs of intrusion attempts (based on complexity of the systems and the level of risk exposure). Automated intrusion detection systems should be updated and supplemented with manual log reviews, as appropriate.

- *Contact Authorities* - Inform appropriate law enforcement authorities of known or suspected criminal activities pertaining to breaches in information security by filing Suspicious Activity Reports in accordance with the FFIEC agencies' reporting rules. Financial institutions should also notify their primary federal supervisor when they experience material information security problems that have a significant adverse effect on the institution's ability to provide effective and reliable services to customers.

International and Domestic Coordination

It is intended that a similar advisory statement will be issued by the Joint Year 2000 Council, Basel, Switzerland, to international supervisors of banks, securities, insurance activities, and payment systems. In some countries, National Y2K Coordinators are also sponsoring programs to educate public and private sector firms regarding information security threats and vulnerabilities during the century rollover period. In the United States, the FFIEC agencies are working closely with the President's Council on Year 2000 Conversion to address this issue.