NCUA LETTER TO CREDIT UNIONS

NATIONAL CREDIT UNION ADMINISTRATION
1775 Duke Street, Alexandria, VA

DATE: July 2002 **LETTER NO.: 02-CU-12**

TO: Federally Insured Credit Unions

SUBJ: Security Program

ENCL: Security Program Considerations

The tragic events of September 11, 2001 and subsequent efforts to improve homeland security have taken much of our focus and attention in recent months. However, despite the critical nature of this undertaking, it is still very important that credit unions not lose sight of physical security considerations. Robberies in credit unions have more than doubled in the last 10 years, and during 2001, 510 credit unions were robbed. Among the risks a financial institution faces, robbery is one of the few that also carries the potential for personal injury. This possibility underscores the importance of a well-structured, effectively-operating security program.

Regulatory Compliance

Part 748 of the National Credit Union Administration's Rules and Regulations requires each federally-insured credit union to have a written security program. The regulation requires the security program be designed to protect credit union offices, ensure the security and confidentiality of member records, assist in identifying persons who commit or attempt crimes, and prevent destruction of vital records.

The chairperson of the credit union's board of directors is required to certify compliance with Part 748 each year. The statement of compliance is provided at the bottom of the Report of Officials form that is submitted annually to the regional director following the credit union's election of officials. In the case of federally-insured state-chartered credit unions, this statement can be mailed to the regional director via the state supervisory authority. The responsibility for providing adequate safeguards to discourage robberies, burglaries, and larcenies and assist in the identification and apprehension of persons who commit such crimes is important, and this certification should be carefully considered each year.

Security Program

You should periodically (at least annually) review the written security program and ensure it is comprehensive in providing for protection of physical assets and personnel.

When reviewing your security program, consider items that are beyond the basic concerns. For example, if your credit union provides the service of safe deposit boxes, there should be a specific security program that addresses the specific risks associated with this service.

The following items should be considered in formulating or revising a security program:

- Procedures for opening and closing for business;
- Procedures for the safekeeping of all currency, negotiable securities, and other valuables;
- Initial and periodic training of employees regarding their responsibilities under the security program and in proper conduct during and after a burglary, robbery, or larceny;
- Procedures for selecting, testing, operating, and maintaining appropriate security devices; and
- Procedures that will assist in identifying persons that commit burglary, robbery, or larceny (e.g., use of camera to record office activity, bait money, chemical and electronic devices).

Security Devices

Just as electronic advancements have increased the protection capacity of security systems, they have also increased the power of anti-security devices. Officials and staff should consider replacing outdated devices and installing any needed equipment. Consideration should be given to:

- A means of protecting cash and other assets (i.e., a vault or safe);
- A lighting system for illuminating the vault during the hours of darkness;
- An alarm system or other appropriate device for promptly notifying law enforcement officials; and
- Tamper-resistant locks on exterior doors and windows that may be opened.

Risk Considerations

All considerations, beyond those required by law or statute, should be based on the potential for risk. The following considerations should be given when implementing a security program and evaluating security devices:

- Incidence of crimes against financial institutions in the area;
- Amount of currency and other valuables exposed to robbery, burglary, or larceny;

- Distance of the office from the nearest law enforcement officers;
- Other security measures in effect at the office;
- Physical characteristics of the office and its surroundings; and
- Cost of the security devices.

Post-Event Procedures

Not all crimes can be prevented. Despite the installation of security devices and the development of security programs, robbery and burglary are inherent risks in financial institutions. Thus, it is important to have an established set of emergency procedures in the event a crime occurs.

As with most forms of emergency preparation, the more you consider when developing your written policies and the more frequently you test the written procedures, the better prepared you will be in the event the situation occurs. Emergency preparation programs and training should include notification procedures, evidence control (in the case of a crime), property control, news media communications, and member inquiries.

Training Information

Above all, the need to provide training to staff is crucial. Inadequate employee training could easily nullify the most comprehensive and detailed security program. Not only does proper training reduce the chances of the occurrence of a robbery or burglary and increase the chances for recovery of stolen assets, it significantly decreases the likelihood of the occurrence resulting in physical harm to your employees.

Many forms of security training are available for both officials and staff. Credit union leagues and various consulting firms offer written guidance and training seminars in developing a successful security program. This information covers many situations including bomb threats, burglary, robbery, disaster recovery, emergency procedures, evacuation procedures, criminal identification practices, extortion threats, and emotional response training for post-trauma situations.

Program Maintenance

Attached you will find a list of questions regarding security. You may want to use these questions as a starting point to identify any potential weaknesses in your current program and as one of your assessment tools when you perform your periodic program review. During your security assessment we recommend you consider the trends in financial crimes, the constant innovations in technology, and the changes occurring within your credit union (branches, ATMs, safe deposit boxes, etc.).

If you add or upgrade security devices or procedures, make your efforts visible and convincing. Emphasizing your efforts could possibly thwart a would-be

robber, and it will provide an increased sense of security for your members and your staff.

I encourage you to please take this opportunity to seriously consider and address the potential security risks which exist for your credit union and staff.

Sincerely,

/S/

Dennis Dollar
Chairman

Enclosure

Security Program Considerations

1. Has the board of directors designated an individual who is charged with the responsibility for the installation, maintenance, and operation of security devices and for the development and administration of a security program that protects the assets and records of the credit union?

2. Has the security officer surveyed the need for security devices in each of the credit union's offices and provided for the installation, maintenance, and operation of:
   (a) A lighting system for illuminating, during the hours of darkness, the area around the vault, if the vault is visible from outside the office?
   (b) Tamper-resistant locks on exterior doors and exterior windows?
   (c) An alarm system or other device for promptly notifying law enforcement officers of an attempted or perpetrated robbery or burglary?

3. Is the credit union's security program:
   (a) Reduced to writing?
   (b) Approved by the board of directors?
   (c) Reviewed at least annually?

4. Does the credit union's security program provide for:
   (a) a designated officer or other employee responsible for ensuring that all security devices are inspected, tested, and serviced on an established schedule and for keeping records of such inspections, testings, and servicings to keep devices in good working order?
   (b) Currency to be kept at a reasonable minimum at each office and at each teller's station or window?
   (c) Procedures for safely removing excess currency and negotiable securities to a locked safe, vault, or other protected place?
   (d) "Bait" money at each teller's station or window?
   (e) Records regarding "bait" money (denominations, bank of issue, serial numbers, series years) verified by a second individual and kept in a safe place?
   (f) Putting currency and negotiable securities in a vault or safe at the earliest time practicable after business hours?
   (g) Locking the vault or safe at the earliest practical time after business hours and opening the vault or safe at the latest practical time before business hours?
   (h) Where practicable, the designation of a person or persons to:
      - Open each office?
      - Inspect the premises to ascertain that no unauthorized persons are present?
      - Signal other employees that the premises are safe before permitting them to enter?

- Ensure that all security devices are turned on and are operating during the periods in which such devices are intended to be used?
- Inspect after closing all areas of each office where currency and negotiable securities are normally handled or stored, in order to ensure that currency and negotiable securities have been put away, that no unauthorized persons are present in such areas, and that the vault or safe and all doors and windows are securely locked?

(i) Training and periodic retraining of employees in their responsibilities under the security program including:
- the proper use of security devices?
- proper employee conduct during and after a robbery?

5. Are currency, savings bonds, travelers checks, and other similar items kept from public view?

6. Is there fixed responsibility for control of keys to office buildings?