NCUA LETTER TO CREDIT UNIONS

NATIONAL CREDIT UNION ADMINISTRATION
1775 Duke Street, Alexandria, VA

DATE: **August 2001** **LETTER NO.: 01-CU-11**

TO: **Federally Insured Credit Unions**

SUBJ: **Electronic Data Security Overview**

ENCL: **Electronic Data Security Overview**

In response to the Gramm-Leach-Bliley Act (GLBA), the National Credit Union Administration (NCUA) recently issued a revision to the NCUA Rules & Regulations Part 748, *Security Program, Report of Crime and Catastrophic Act and Bank Secrecy Act Compliance*. The change to the regulation itself was minimal; however, the NCUA incorporated an appendix entitled "*Guidelines for Safeguarding Member Information"* to assist credit unions in determining how to best protect their members' data. While Part 748 addresses both the physical protection and electronic protection of member information, the enclosure to this letter, *Electronic Data Security Overview*, focuses primarily on the electronic aspects of member data security. The enclosure discusses how to develop and implement a security program for electronic data and information systems. This letter and its attachment assist the NCUA in meeting the requirements of Title V, Subtitle A, of the GLBA.

If you have any questions or concerns, please contact your NCUA Regional Office or State Supervisory Authority.

Sincerely,

/s/

Dennis Dollar
Acting Chairman

Enclosure

Electronic Data Security Overview

Part 748.0 Security Program

Part 748.0 of the Rules & Regulations requires each federally-insured credit union to develop a written security program. This program must address how the credit union will:

1. protect each credit union office from robberies, burglaries, larcenies, and embezzlements;

2. ensure the security and confidentiality of member records, protect against anticipated threats or hazards to the security or integrity of such records, and protect against unauthorized access to or use of such records that could result in substantial harm or serious inconvenience to a member;

3. assist in the identification of persons who commit or attempt such actions and crimes; and

4. prevent destruction of vital records, as defined in 12 CFR Part 749.

The appendix to Part 748 provides guidelines to assist credit unions in meeting the above four criteria. The guidelines are not mandatory; however, they provide a good framework from which you can develop your policies and procedures.

Security Policies and Procedures

As you deploy various systems and services, you must re-evaluate your written security program and make the appropriate adjustments. Depending on the type and level of systems and services you provide, your security program may become difficult to manage effectively. Credit unions in this situation should consider assistance from outside sources such as trade organizations or security specialist firms and organizations.

Large vs. small credit unions. Regardless of the size of your credit union, you must address the security of its systems and the data which resides on, or is transmitted across, those systems. Two credit unions of significantly different asset sizes, which provide services via the Internet, face and must deal with the same risks associated with that service. Each credit union's policies and procedures need to be commensurate not only with the size of the credit union, but also with the complexity of services offered and systems used to deliver those services. Since each credit union operates in its own unique environment, your policies and procedures need to be unique to your situation.

When developing your policies and procedures, you should:

- Identify the services provided and systems (hardware and software) used.
- Identify the risks and threats associated with each system and service.
- Determine the likelihood the risk/threat could occur.
- Identify and evaluate various methodologies to mitigate the risks/threats.
- Develop the policies and procedures to address the risks/threats.
- Monitor and adjust, if necessary, the policies and procedures to achieve the desired results.
- Review policies and procedures at least annually.
- Train and educate staff.

The following is a discussion of the preceding policies and procedures.

Identify systems and services. Before you can determine what kind of risks you are exposed to, you must identify the various hardware and software configurations used to deliver your services (back office operations as well as member services). Most, if not all, credit unions performed this task when addressing the Y2K issue. The purpose behind identifying hardware and software configurations is to determine what issues or weaknesses these systems may have. The best source for this information is the vendor of the product. Many of these vendors maintain websites identifying issues with their products, such as security problems, as well as provide solutions, fixes, updates, and patches. In addition to vendors, there are a host of websites dedicated to providing information concerning hardware and software issues and advisories such as the SANS Institute (www.sans.org), Security Focus (www.securityfocus.com), and Computer Emergency Response Team (CERT, www.cert.org).[1] Credit unions should routinely monitor the website of their vendors, as well as their vendors' newsletters and periodicals, to ensure they have an up-to-date understanding of any issues involving their various hardware and software systems.

Identify the risks and threats. You need to identify reasonably foreseeable internal and external threats based upon the types of systems and services provided. What is reasonably foreseeable depends on the credit union's information technology (IT) environment and the types of services provided. For example, it is reasonably foreseeable that a credit union providing services via the Internet, whether in-house developed or outsourced, could be exposed to hacking, defacement, and denial of services attacks (these are common risks and threats associated with the Internet). Likewise, how those services are deployed will determine the risks and threats a credit union may be exposed to. For example, a credit union providing services via the Internet

[1] NCUA does not endorse these organizations/companies, or others mentioned in this document, or their websites. They are listed as examples only.

and hosting[2] the systems that provide those services will face different risks and threats than one providing similar services but outsourcing the hosting to a vendor.

For each system and service, you should list the risks/threats. You should classify each risk/threat as internal, external, or both. You should determine what impact the risks/threats may have on the credit union such as operational, transactional, reputation, etc., taking into account whether the system, service, or data is critical or non-critical, sensitive or non-sensitive. You should develop an impact ranking system and rank each risk/threat. What type of ranking system employed is determined by you. An example is a Low, Medium, High ranking system.

Determine the likelihood risks/threats could occur. The credit union's IT environment heavily influences the possibility of a particular risk/threat occurring. For example, a credit union providing Internet services with no protection from outside sources (such as a firewall) would face a higher risk of an occurrence than a credit union employing a system protecting their internal environment. Similar to the discussion in the previous section, you should develop a ranking system and rank the likelihood of occurrence for each risk/threat. The combination of the impact ranking with the occurrence ranking provides a total ranking for that risk/threat.

Identify and evaluate various methodologies. Based upon the total ranking for each risk/threat, you should determine what action to take to mitigate the risk/threat. In some cases, you may decide not to take any action at all. In these instances, you should clearly document your reasoning and justification for not taking action. In addition, you should determine whether your insurance coverage may be impacted by your decision.

Determining what specific actions to take to mitigate a risk/threat depends upon the type of risk/threat and the systems used to deploy the services. For example, if you determine that you need to protect certain member account information, you may decide to encrypt the data or require strong passwords or authentication before being able to access the data. Other options available to protect systems and data include: intrusion detection, firewalls, virus protection, digital signatures, certificates of authority, as well as how a credit union structures its IT topology[3].

Develop the policies and procedures. Once you know what you need to protect, why you need to protect it, and how best to protect it, you are in a position to develop adequate policies and procedures. Policies should be sufficient to address who, what, when, and why; while procedures should be sufficient to address how. Policies set the framework from which procedures are derived. Actual policy development is beyond the scope of this letter; however, abundant sources of policy and procedure development

[2] Hosting means providing the service. Hosting may include only providing the hardware, software, content, or any combination thereof.

[3] IT topology refers to how systems are linked to one another and how data flows between the various systems.

information exist such as other credit unions, trade organizations, specialized firms and organizations, and the Internet.

Monitor and adjust policies and procedures. Changes to your IT environment can drastically impact your security. As you deploy or remove systems and/or services, your security policy and procedures need to be adjusted. In addition, new threats arise almost daily requiring you to stay informed and take quick action. A well designed security policy will address security concerns and issues at a level which will minimize the need for constant updating. However, you will need to update your security procedures and practices frequently to keep pace with your changing IT environment. How often you need to update your policies, procedures, and practices depends upon your environment. For credit unions operating in a closed environment[4], the need to revise and update policies and procedures may not be as often as one which operates in an open environment[5].

Review policies and procedures. The Supervisory Committee should include a review of the credit union's security policies and procedures. How often they conduct the review should be based upon the level of risk you have assumed and how effectively you have managed that risk. In some cases, an annual review, generally part of the annual audit, is sufficient. In other cases, a more frequent review may be warranted such as when the credit union's IT environment significantly changes or new services are implemented. The Supervisory Committee's role is to assure that controls are adequate to safeguard member information and that practices comply with policies and procedures. Whether part of the annual report, or performed as a separate review, the Supervisory Committee should provide a report of their findings to the board of directors.

Train and educate staff. Policies and procedures are of minimal benefit unless staff know they exist and understand them. To ensure staff acceptance and participation, the purpose of the policies and procedures should be discussed with credit union staff. In addition, staff should be fully aware of their responsibilities in order to accomplish their tasks related to the policies and procedures. As part of an ongoing training program, you should provide staff with annual policy updates and consider having each employee sign a security acknowledgment form.

Other Considerations

Outsourcing. Many credit unions contract with a vendor (outsource) for some or all of their IT needs. Outsourcing one or more services does not alleviate your responsibility for ensuring that your systems and member data are secure. You need to ensure that your vendors implement security programs which meet your standards. To determine if

[4] A closed environment is one in which primarily only credit union employees, its vendors, or other authorized 3rd parties have access to the credit union's information systems.

[5] An open environment is one in which external parties may gain access to credit union systems (i.e. via the Internet).

a vendor's security program is sufficient, you should ensure contracts specify who (the credit union or vendor) is responsible. You should carefully review the service level agreements contained in your vendor contracts to determine what services will be provided, under what conditions they will be provided, when they will be provided, and how they will be provided. In addition, you should review audit reports (such as SAS 70 reviews, internal audits, 3rd party audits) of your vendors. Prior to entering into a contract with a vendor, you should inquire about the vendor's security program, their level of risk tolerance, their procedures for addressing risks and threats (such as how often does the vendor install updates, patches, and fixes to their systems; do they have established and tested procedures for dealing with incidents; etc.), and their procedures for notifying customers should a problem arise. For more information concerning outsourcing management, see NCUA Letter to Credit Union #00-CU-11 Risk Management of Outsourced Technology Services.

Security Committee. Where practical, you should establish a security committee or team assigned with the responsibility of developing, implementing, monitoring, and revising security policies and procedures. Team members should include representatives from senior management, information technology department, human resources/personnel department, legal department, and customer service department. Having such a diversified team will allow for input from different perspectives and the development of effective policies and procedures.

Summary

Whether or not a credit union has an Internet presence, such as a website, it still has an obligation to protect its members' data. In the past, credit unions generally needed to focus on internal threats because they processed and stored member information in a closed environment. However, as credit unions provide members with access to their accounts via the Internet, they assume more risk and face a constantly changing environment.