I. INTRODUCTION

Purpose and Scope of the IT Security Compliance Guide

This IT Security Compliance Guide[1] is intended to help credit unions[2] comply with the *Interagency Guidelines Establishing Information Security Standards* (NCUA Rules & Regulations, Part 748, Appendix A&B). The guide summarizes the obligations of credit unions to protect information, and illustrates how certain provisions of the National Credit Union Administration Rules and Regulations, Part 748, Appendix A & B (Security Guidelines) apply to specific situations. The appendix lists resources that may be helpful in assessing risks and designing and implementing information security programs.

Although this guide was designed to help credit unions identify and comply with the requirements of the Security Guidelines, it is not a substitute for the Security Guidelines. Moreover, this guide only addresses obligations of credit unions under the Security Guidelines and does not address the applicability of any other federal or state laws or regulations that may pertain to policies or practices for protecting records and information.

Background and Overview of Security Guidelines

The Security Guidelines implement section 501 and 505(b) of the Gramm-Leach-Bliley Act (GLB Act)[3] and section 621(b) and 628 of the Fair and Accurate Credit Transactions Act of 2003 (FACT Act).[4] The Security Guidelines establish standards relating to administrative, technical, and physical safeguards to ensure the security, confidentiality, integrity and the proper disposal of information.

Each of the requirements in the Security Guidelines regarding the proper disposal of information also apply to personal information a credit union obtains about individuals regardless of whether they are the credit union’s members ("consumer information"). Consumer information includes, for example, a credit report about an individual who applies for but does not obtain a loan, an individual who guarantees a loan, and an employee or prospective employee. A credit union must require its service providers that have access to consumer information, by contract, to develop appropriate measures for the proper disposal of the information.

[1] The guide is issued in accordance with the Small Business Regulatory Enforcement Fairness Act of 1996, Pub. L. No. 104-121, 110 Stat. 857, *reprinted in* 5 U.S.C.A. § 601, note (West Supp. 2004).

[2] This guide applies to federally-insured credit unions (NCUA).

[3] 15 U.S.C. § 6801. and 6805(b)

[4] 15 U.S.C. § 1681s(b) and 1681w.

Under the Security Guidelines, each credit union must:

- Develop and maintain an effective information security program tailored to the complexity of its operations, and

- Require its service providers that have access to a credit union's information, by contract, to take appropriate steps to protect the security and confidentiality of this information.

The standards set forth in the Security Guidelines are consistent with the long-standing principles the Agency follow when examining the security programs of credit unions. Each credit union must identify and evaluate risks to its information, develop a plan to mitigate the risks, implement the plan, test the plan, and monitor the need to update the plan**.**

Distinction between the Security Guidelines and the Privacy Rule

The requirements of the Security Guidelines and the NCUA regulations regarding financial privacy (Privacy Rule)[5] both relate to the confidentiality of information. However, they differ in the following key respects:

- The Security Guidelines address safeguarding the confidentiality and security of information and ensuring the proper disposal of information. They are directed toward preventing or responding to foreseeable threats to, or unauthorized access or use of, that information. The Security Guidelines provide that credit unions must contractually require their affiliated and non-affiliated third party service providers that have access to the credit union's information to protect that information.

- The Privacy Rule limits a credit union's disclosure of nonpublic personal information to unaffiliated third parties, such as by selling the information to unaffiliated third parties. Subject to certain exceptions, the Privacy Rule prohibits disclosure of a consumer's nonpublic personal information to a unaffiliated third party unless certain notice requirements are met and the consumer does not elect to prevent, or "opt out of," the disclosure.[6] The Privacy Rule requires that privacy notices provided to members and consumers describe the credit union's policies and practices to protect the confidentiality and security of that

[5] The National Credit Union Administration (NCUA) has issued privacy regulations that implement sections 502-509 of the GLB Act; the National Credit Union Administration Rules and Regulations, Part 716.

[6] The Privacy Rule defines a "consumer" to mean an individual who obtains or has obtained a financial product or service that is to be used primarily for personal, family, or household purposes. For example, an individual who applies to a credit union for credit for personal purposes is a consumer of a financial service, regardless of whether the credit is extended. Privacy Rule § 716.3(e) (1).

information. It does not impose any other obligations with respect to safeguarding members' or consumers' information.

II. IMPORTANT TERMS USED IN THE SECURITY GUIDELINES

Information

The Security Guidelines require credit unions to safeguard and properly dispose of any record containing nonpublic personal information about an individual who has obtained a financial product or service from the credit union that is to be used primarily for personal, family, or household purposes, and who has an ongoing relationship with the institution. Information is defined as any record containing nonpublic personal information, as defined in 12 CFR 716.3(q), about a member whether in paper, electronic, or other form, that is maintained by or on behalf of the credit union.

Information Systems

Member information systems means any method used to access, collect, store, use, transmit, protect, or dispose of information.[7] Member information systems encompass all the hardware and software a credit union uses to access, collect, store, use, transmit, protect, or dispose of information. The Security Guidelines apply specifically to these information systems because information will be at risk if one or more of the components of those systems are compromised.

Information Security Program

An *information security program* is the written plan created and implemented by a credit union to identify and control risks to information and information systems and to properly dispose of information. The plan includes policies and procedures regarding the institution's risk assessment, controls, testing, service-provider oversight, periodic review and updating, and reporting to its board of directors.

Service Providers

Service provider means any person or entity that maintains, processes, or otherwise is permitted access to member information through its provision of services directly to the credit union.[8]

For example, a processor that directly obtains, processes, stores, or transmits information on a credit union's behalf is its service provider. Similarly, an attorney, accountant, or consultant who performs services for a credit union and has access to information is a service provider for the credit union.

[7] NCUA Rules and Regulations, Part 748, Appendix A, Section I.B.2.e.

[8] NCUA Rules and Regulations, Part 748, Appendix A, Section I.B.2.f.

III. DEVELOPING AND IMPLEMENTING AN INFORMATION SECURITY PROGRAM

The Security Guidelines[9] requires credit unions to implement an information security program that includes administrative, technical, and physical safeguards designed to achieve the following objectives:

- Ensure the security and confidentiality of member information;

- Protect against any anticipated threats or hazards to the security or integrity of such information;

- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any member; and

- Ensure the proper disposal of member and consumer information.

To achieve these objectives, an information security program must suit the size and complexity of a credit union's operations and the nature and scope of its activities.

The various business units or divisions of the credit union are not required to create and implement the same policies and procedures. If the business units have different security controls, the credit union must include them in its written information security program and coordinate the implementation of the controls so as to safeguard and ensure the proper disposal of member information throughout the credit union.

Implementing an information security program begins with conducting an assessment of reasonably foreseeable risks. Like other elements of an information security program, risk assessment procedures, analysis, and results must be written.

Under the Security Guidelines, a risk assessment must include the following four steps:

- Identifying reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of member information or member information systems;

- Assessing the likelihood and potential damage of identified threats, taking into consideration the sensitivity of the member information;

- Assessing the sufficiency of the policies, procedures, member information systems, and other arrangements in place to control the identified risks; and

[9] NCUA Rules and Regulations, Part 748, Appendix A, Section II, A & B.

- Applying each of the foregoing steps in connection with the disposal of information.

Identifying Reasonably Foreseeable Internal and External Threats

A risk assessment must be sufficient in scope to identify the *reasonably foreseeable* threats from within and outside a credit union's operations that could result in unauthorized disclosure, misuse, alteration, or destruction of information or information systems, as well as the reasonably foreseeable threats due to the disposal of member information. The scale and complexity of its operations and the scope and nature of a credit union's activities will affect the nature of the threats a credit union will face.

For example, a credit union should review the structure (topology) of its computer network to determine how its computers are accessible from outside the credit union. If the computer systems are connected to the Internet or any outside party, a credit union's assessment should address the reasonably foreseeable threats posed by that connectivity.

The risk assessment also should address the reasonably foreseeable risks to:

- member information that is stored on systems owned or managed by service providers, and

- member information disposed of by service providers used by the credit union.

Assessing the Likelihood and Potential Damage of Identified Threats

In addition to identifying reasonably foreseeable threats to member information and member information systems and to member information that a credit union disposes, a risk assessment must evaluate the potential damage from these threats. The Security Guidelines allow broad latitude to determine the sensitivity of member information in the course of assessing the likelihood of, and potential damage from, the identified threats.

For example, to determine the sensitivity of member information, a credit union could develop a framework that analyzes the relative value of this information to its members based on whether improper access to, or loss of, the information would result in harm or inconvenience to them.

In the course of assessing the potential threats identified, a credit union should consider its ability to identify unauthorized changes to records. In addition, it should take into consideration its ability to reconstruct the records from duplicate records or backup information systems.

Assessing the Sufficiency of Policies and Procedures

Evaluating the sufficiency of policies and procedures is a key element of a credit union's risk assessment. The evaluation process includes identifying weaknesses or other deficiencies in existing security controls and assessing to what extent member information and member information systems are at risk as a result of those weaknesses and to what extent member information is at risk as a result of improper methods of disposal.

The risk assessment may include an automated analysis of the vulnerability of certain information systems. However, an automated analysis likely will not address manual processes and controls, detection of, and response to, intrusions into information systems, physical security, employee training, and other key controls. Accordingly, an automated analysis of vulnerabilities should be only one tool used in conducting a risk assessment.

When performing a risk assessment, a credit union may want to consult the resources and standards listed in the appendix to this guide, and consider incorporating the practices developed by the listed organizations when developing its information security program.[10]

Hiring an Outside Consultant to Conduct the Risk Assessment

A credit union may elect to hire an outside consultant to conduct the risk assessment of its information security program, but it nevertheless remains responsible for the adequacy of the assessment and the analysis that will necessarily flow from it. Therefore, the credit union must ensure that the assessment specifically examines the risks that relate to *its* member information, member information systems and systems for disposal of member information.

For example, a generic assessment that describes vulnerabilities commonly associated with the various systems and applications used by the credit union would be inadequate. The assessment should take into account the particular configuration of the institution’s systems and the nature of its business.

Where an outside consultant has only examined a subset of the institution’s risks, such as risks to computer systems, the credit union will need to supplement the outside consultant’s assessment by examining its other risks, such as risks to records maintained in paper form, to satisfy the requirements of the Security Guidelines. *For example,* a credit union should evaluate the other controls put into place, such as the security of member information in cabinets and vaults.

Management must review the risk assessment and use that assessment as an integral component of its information security program to guide the development of or adjustments to the credit union’s information security program.

[10] Credit unions also may want to consult the FFIEC Agencies’ guidance regarding risk assessments as described in the Information Security Booklet.

Engaging in an Ongoing Risk Assessment Process

Risk assessment is an ongoing process. Credit unions should continually review their current policies and procedures to make certain they are adequate to safeguard member information and member information systems, ensure the proper disposal of member information, and include in their written information security program both their review and their findings. The risk assessment must be updated, as necessary, to account for system changes before they are implemented or new products or services before they are offered.

IV. DESIGNING SECURITY CONTROLS

The Security Guidelines require a credit union to design an information security program to control the risks identified through its assessment, commensurate with the sensitivity of the information and the complexity and scope of its activities. Thus, a credit union must consider a variety of policies, procedures, and technical controls and adopt those measures that it determines appropriately address the identified risks.

The Security Guidelines provide a list of measures that a credit union consider and, if appropriate, adopt. These are:

- Access controls on member information systems, including controls to authenticate and permit access only to authorized individuals, and controls to prevent employees from providing member information to unauthorized individuals who may seek to obtain this information through fraudulent means;

- Access restrictions at physical locations containing member information, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals;

- Encryption of electronic member information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access;

- Procedures designed to ensure that member information system modifications are consistent with the credit union’s information security program;

- Dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for, or access to, member information;

- Monitoring systems and procedures to detect actual and attempted attacks on, or intrusions into, member information systems;

- Response programs that specify actions to be taken when the credit union suspects or detects that unauthorized individuals have gained access to member information systems, including appropriate reports to regulatory and law enforcement agencies; and

- Measures to protect against destruction, loss, or damage of member information due to potential environmental hazards, such as fire and water damage or technological failures.

The Security Guidelines recommends a credit union consider whether it should adopt controls to authenticate and permit only authorized individual's access to certain forms of information.[11] Under this security control, a credit union should consider the need for a firewall for their network. If a credit union maintains any sort of Internet or other external connectivity, its systems may require multiple firewalls of adequate capacity that are properly placed and appropriately configured.

Similarly, a credit union should consider whether the encryption of member information that is maintained in electronic form is warranted in light of its risk assessment. If it is warranted, the credit union must adopt appropriate encryption measures, such as measures that protect information in transit or in storage, or both.[12] However, the Security Guidelines do not impose any specific authentication[13] or encryption standards.

A credit union should consider the use of an intrusion detection system to alert it to attacks on computer systems that store member information.[14] In assessing the need for such a system, a credit union should evaluate the ability of its staff to rapidly and accurately identify an intrusion and the damage that could occur between the time an intrusion occurs and the time the intrusion is recognized and action is taken.

Credit unions should develop, implement, and maintain, as part of its information security program, appropriate measures to properly dispose of member information in accordance with each of the requirements of the Security Guidelines.[15] Although the Security Guidelines do not prescribe a specific method of disposal, the NCUA expects credit unions to have appropriate risk-based disposal procedures for their records.

A credit union should:

- Ensure that paper records containing member information are rendered unreadable, such as by shredding or any other means; and

[11] NCUA Rules and Regulations, Part 748, Appendix A, Section III.C.1.a.

[12] NCUA Rules and Regulations, Part 748, Appendix A, Section III.C.1.c.

[13] NCUA issued a Letter to Credit Union 05-CU-18 dated November 2005 addressing Guidance on Authentication in Internet Banking Environment. This was an update to Letter to Credit Union 01-CU-10 published in August 2001, Authentication in an Electronic Banking Environment.

[14] NCUA Rules and Regulations, Part 748, Appendix A, Section III.C.1.f.

[15] NCUA Rules and Regulations, Part 748, Appendix A, Section III.C.4.

- Recognize that computer-based records present unique disposal problems. Residual data frequently remains on media after erasure. Since that data can be recovered, additional disposal techniques should be applied to sensitive electronic data.

In addition to considering the measures recommended by the Security Guidelines, each credit union may need to implement additional, procedures, or controls specific to the nature of its operations. A credit union may implement safeguards designed to provide the same level of protection to all member information, provided that the level is appropriate for the most sensitive classes of information.

Insurance coverage is not a substitute for an information security program. Although insurance may protect a credit union or its members against certain losses associated with unauthorized disclosure, misuse, alteration, or destruction of information, the Security Guidelines recommend a credit union implement and maintain controls designed to prevent those acts from occurring.

Develop and Implement A Response Program

The NCUA Rules and Regulation Part 748, Appendix B was issued to require programs to respond to unauthorized access to member information. According to Appendix B, credit union's information security program should include a response program to address unauthorized access to, or use of, sensitive member information that could result in substantial harm or inconvenience to a member.

The components of an effective response program should include at a minimum:

- Assessment of the nature and scope of the incident and identification of what member information and types of member information has been accessed or misused;

- Prompt notification to its primary federal regulator, and, in the case of state-chartered credit unions, its applicable state supervisory authority, once the credit union becomes aware of an incident involving unauthorized access to, or use of, sensitive member information;

- Notification to appropriate law enforcement authorities, in addition to filing a timely Suspicious Activity Report, in situations involving Federal criminal violations requiring immediate attention;

- Measures to contain and control the incident to prevent further unauthorized access to, or misuse of, member information, while preserving records and other evidence; and

- Notification to members when warranted.

Circumstances for Member Notice

Appendix B Guidance describes when and how a credit union should provide notice to members affected by unauthorized access or misuse of sensitive member information. In particular, it indicates that:

- Once the credit union becomes aware of an incident of unauthorized access to sensitive information, it should conduct a reasonable investigation to determine promptly the likelihood that the information has been, or will be, misused.

- If the credit union determines that misuse of member information has occurred or is reasonably possible, it should notify any affected member as soon as possible.[16]

Sensitive information means:

- A member's name, address, or telephone number, in conjunction with the member's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the member's account; or

- Any combination of components of information that would allow an unauthorized third party to log onto or access the member's account electronically, such as user name and password, or password and account number.

V. TRAINING STAFF

The Security Guidelines recommends a credit union train staff to prepare and implement its information security program.[17] The credit union should consider providing specialized training to ensure that personnel sufficiently protect member information in accordance with its information security program.

For example, a credit union should:

- Train staff to recognize and respond to schemes to commit fraud or identity theft, such as by guarding against pretext calling;[18]

- Provide staff members responsible for building or maintaining computer systems and local and wide-area networks with adequate training, including instruction about

[16] Appendix B of Part 748 of the NCUA Rules and Regulations recognizes that member notice may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the credit union with a written request for the delay. However, the credit union should notify its members as soon as notification will no longer interfere with the investigation.

[17] NCUA Rules and Regulations, Part 748, Appendix A, Section III.C.2.

[18] *See* Letter to Credit Union 01-CU-09, Identity Theft and Pretext Calling published in September 2001.

computer security; and

- Train staff to properly dispose of member information.

VI. TESTING KEY CONTROLS

The Security Guidelines recommends a credit union test the key controls, systems, and procedures of its information security program.[19] The credit union's risk assessment should determine the scope, sequence, and frequency of testing.

The NCUA expects testing to be done on a regular basis and at a frequency that takes into account the rapid evolution of threats to computer security. Testing may vary over time depending, in part, on the adequacy of any improvements a credit union implements to prevent access after detecting an intrusion. Independent third parties or staff, other than those who develop or maintain the institution's security programs, must perform or review the testing.

VII. OVERSEEING SERVICE PROVIDERS

The Security Guidelines set forth specific requirements that apply to a credit union's arrangements with service providers. A credit union should:

- Exercise appropriate due diligence in selecting its service providers;

- Require its service providers by contract to implement appropriate measures designed to meet the *objectives* of the Security Guidelines; and

- Where indicated by its risk assessment, monitor its service providers to confirm that they have satisfied their obligations under the contract described above.

As stated in section II of this guide, a service provider is *any* party that is permitted access to a credit union's information through the provision of services directly to the credit union. Examples of service providers include a person or corporation that tests computer systems or processes members' transactions on the credit union's behalf, document-shredding firms, Internet banking service providers, and computer network management firms.

Contracts With Service Providers

The contract provisions in the Security Guidelines apply to *all* of a credit union's service providers. After exercising due diligence in selecting a company, the credit union must enter into and enforce a contract with the company that requires it to implement

[19] NCUA Rules and Regulations, Part 748, Appendix A, Section C.3.

appropriate measures designed to implement the *objectives* of the Security Guidelines.[20]

In particular, credit unions must require their service providers by contract to:

- Implement appropriate measures designed to protect against unauthorized access to or use of member information maintained by the service provider that could result in substantial harm or inconvenience to any member; and

- Properly dispose of member information.

In addition, the Incident Response Guidance states that a credit union's contract with its service provider should require the service provider to take appropriate actions to address incidents of unauthorized access to the credit union's[21] information, including notification to the credit union as soon as possible following any such incident.

Monitoring Service Providers

A credit union should monitor each of its service providers in accordance with its risk assessment of the hazards posed by the providers. However, the Security Guidelines do not impose any specific requirements regarding the methods or frequency of monitoring service providers to ensure that they are fulfilling their contractual obligations.

To the extent that monitoring is warranted, a credit union must confirm that the service provider is fulfilling its obligations under its contract, such as by reviewing audits, summaries of test results, or equivalent evaluations of its work. These audits, tests, or evaluations should be conducted by a qualified party independent of management and personnel responsible for the development or maintenance of the service provider's security program.

The reports of test results may contain proprietary information about the service provider's systems or they may include non-public personal information about members of another credit union. Under certain circumstances it may be appropriate for service providers to redact confidential and sensitive information from audit reports or test results before giving the credit union a copy. Where this is the case, a credit union should make sure that the information is sufficient for it to conduct an accurate review, that all material deficiencies have been or are being corrected, and that the reports or test results are timely and relevant,

[20] The third-party-contract requirements in the Privacy Rule are more limited than those in the Security Guidelines. When a credit union relies on the "opt out" exception for service providers and joint marketing described in §716.13 of the Privacy Rule (as opposed to other exceptions), in order to disclose nonpublic personal information about a consumer to a nonaffiliated third party without first providing the consumer with an opportunity to opt out of that disclosure, it must enter into a contract with that third party. The contract must generally prohibit the nonaffiliated third party from disclosing or using the information other than to carry out the purposes for which the information was disclosed.

[21] NCUA Rules and Regulations, Part 748, Appendix B, Section C.

The credit union should include reviews of its service providers in its written information security program.

VIII. ADJUSTING THE PROGRAM

A credit union should adjust its information security program to reflect the results of its ongoing risk assessment and the key controls it identifies as necessary to safeguard member information and ensure the proper disposal of member information. It should adjust the program to take into account changes in technology, the sensitivity of its member information, internal or external threats to information, and the credit union's own changing business arrangement such as mergers, acquisitions, alliances and joint ventures, outsourcing arrangements, and changes in member information systems.

For example, a credit union should ensure that its policies and procedures regarding the disposal of member information are adequate should it decide to close or relocate offices, because such a change in business arrangements may involve disposal of a larger volume of records than in the normal course of business.

IX. RESPONSIBILITIES OF AND REPORTS TO THE BOARD OF DIRECTORS

Under the Security Guidelines, a credit union's board of directors, or an appropriate committee of the board, must satisfy specific requirements designed to ensure that the credit union's information security program is developed, implemented, and maintained under the supervision of those who are ultimately responsible. At the outset, the board, or appropriate committee, should approve the written information security program. Thereafter, the board or appropriate committee must oversee the implementation and maintenance of the program. These duties include assigning specific responsibility for implementing the program and reviewing reports prepared by management.[22]

Correspondingly, management must provide a report to the board, or an appropriate committee, at least annually that describes the overall status of the information security program and compliance with the Security Guidelines. The reports should describe material matters relating to the program.

For example, whether a credit union conducts its own risk assessment or hires another person to conduct it, the results of that assessment should be reported to the board or an appropriate committee.

The Security Guidelines provide an illustrative list of other material matters that may be appropriate to include in the report, such as decisions about risk management and control arrangements with service providers, results of testing, security breaches or violations

[22] NCUA Rules and Regulations, Part 748, Appendix A, Section III.A.

and management's responses, and recommendations for changes in the information security program.[23]

[23] NCUA Rules and Regulations, Part 748, Appendix A, Section III.F.

APPENDIX

Note: This list of resources is intended to further assist credit unions in complying with the National Credit Union Administration Rules and Regulations, Part 748, Appendix A & B. The listed organizations provide information on computer security, with a focus on risk-assessment methodologies and the design and implementation of computer security programs. Any mention of a commercial product is for information purposes only and does not imply a recommendation or endorsement by the NCUA.

Center for Internet Security (CIS) – A nonprofit cooperative enterprise that helps organizations reduce the risk of business and e-commerce disruptions resulting from inadequate security configurations. CIS develops security benchmarks through a global consensus process. Its members include the American Institute of Certified Public Accountants (AICPA), Financial Management Service of the U.S. Department of the Treasury, and Institute for Security Technology Studies (Dartmouth College). www.cisecurity.org

CERT Coordination Center – A center for Internet security expertise operated by Carnegie Mellon University. CERT provides security-incident reports, vulnerability reports, security-evaluation tools, security modules, and information on business continuity planning, intrusion detection, and network security. It also offers training programs at Carnegie Mellon. CERT has developed an approach for self-directed evaluations of information security risk called Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE). www.cert.org/octave/

Information Systems Audit and Control Association (ISACA) – An association that develops IT auditing and control standards and administers the Certified Information Systems Auditor (CISA) designation. ISACA developed Control Objectives for Information and Related Technology (COBIT) as a standard for IT security and control practices that provides a reference framework for management, users, and IT audit, control, and security practitioners. www.isaca.org/cobit.htm

International Organization for Standardization (ISO) – A network of national standards institutes from 140 countries. Published *ISO/IEC 17799:2000, Code of Practice for Information Security Management*. www.iso.org. Interested parties should also review the *Common Criteria for Information Technology Security Evaluation*. http://www.commoncriteriaportal.org/public/expert/index.php?menu=3

Internet Security Alliance (ISA) – A collaborative effort between Carnegie Mellon University's Software Engineering Institute, the university's CERT Coordination Center, and the Electronic Industries Alliance (a federation of trade associations). ISA provides access to information on threats and vulnerability, industry best practices, and developments in Internet security policy. www.isalliance.org

Institute for Security Technology Studies (Dartmouth College) – An institute that studies and develops technologies to be used in counter-terrorism efforts, especially in the areas of threat characterization and intelligence gathering, threat detection and interdiction, preparedness and protection, response, and recovery. The institute publishes a daily news summary titled *Security in the News*, offers on-line training courses, and publishes papers on such topics as firewalls and virus scanning. The web site includes worm-detection tools and analyses of system vulnerabilities. www.ists.dartmouth.edu

National Institute of Standards and Technology (NIST) – An agency within the U.S. Commerce Department's Technology Administration that develops and promotes measurements, standards, and technology to enhance productivity. NIST operates the Computer Security Resource Center, which is dedicated to improving information systems security by raising awareness of IT risks, researching vulnerabilities, and developing standards and tests to validate IT security. Four particularly helpful documents are: *Special Publication 800-14,Generally Accepted Principles and Practices for Securing Information Technology Systems; Special Publication 800-18, Guide for Developing Security Plans for Information Technology Systems; Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems; Special Publication 800-30, Risk Management Guide for Information Technology Systems;* and *Federal Information Processing Standards Publication 199, Standards for Security Categorization of Federal Information and Information Systems*. http://csrc.nist.gov. The web site provides links to a large number of academic, professional, and government sponsored web sites that provide additional information on computer or system security.

National Security Agency (NSA) – The National Security Agency/Central Security Service is America's cryptologic organization. It coordinates, directs, and performs highly specialized activities to protect U.S. information systems and produce foreign intelligence information. A high technology organization, NSA is on the frontiers of communications and data processing. The web site includes links to NSA research on various information security topics. www.nsa.gov