

## **1. What is the need for a Financial Services Security Lab?**

- The idea of a laboratory to test security products for electronic banking and commerce began to grow even before the growth in Web-based financial transactions became so prominent. The BITS Security Laboratory is the financial services industry's proactive way of ensuring that safety standards for electronic commerce and banking continue to be strengthened as new technologies are developed and the volume of digital commerce keeps growing. This benefits not only financial services customers, but also the industry, the technology providers, and the government, as it helps protect the nation's critical infrastructure. The establishment of the Security Lab is also one of the most specific ways the industry can move toward meeting the requirements of the Office of the Comptroller of the Currency (OCC) Bulletin (98-38) on technology risk management in PC Banking.

The establishment of the Security Lab is the financial services industry's latest initiative to further ensure secure financial transactions in today's online marketplace. While incidents of cybercrime are often reported in various computer-based scenarios, these do not indicate any particular vulnerability in electronic banking systems. The banking industry brings its historic expertise in assuring safe and sound financial transactions to the new environment of electronic commerce. No other financial services providers have comparable expertise and experience in risk management. Banks put the highest priority on protecting the security and soundness of financial transactions and the systems upon which those transactions depend. The fact that banks have traditionally been highly regulated contributes to this priority.

## **2. How did BITS get involved? Why is it a BITS Financial Services Security Lab?**

- BITS, the technology group for The Financial Services Roundtable, was created in November 1996 to foster the growth and development of electronic banking and commerce in an open environment, and to encourage greater choice and efficiency in financial software, access devices, networks and processing capabilities for the benefit of financial institutions and their customers. It is the only industry organization dedicated solely to leveraging technology and eCommerce for financial services. Security has been a high priority since BITS' inception. BITS has taken a leadership role in this arena on behalf of the financial services industry.

The creation of the BITS Security Lab has been underway for nearly two years and is intended to create a private-sector partnership between Technology Providers and Financial Services Providers focused on enhancing e-commerce security while improving efficiency. It is a BITS Lab because BITS represents the financial services industry rather than an individual client or group.

The Financial Services Roundtable (formerly The Bankers Roundtable) recently broadened its scope to represent all financial services entities. BITS, its technology group, now has a broader mandate as well—to leverage technology and eCommerce for all financial services. Through its various initiatives, BITS has worked in collaboration across industries to promote safety and soundness in payments systems and in electronic banking products, and has a track record of achievement in this arena.

### **3. What is the thinking behind the BITS Tested Mark? What will it mean to a product? To a bank customer?**

- The goal is to provide the industry and consumers with a Universal Labs (UL)-like assurance that products meet a certain level of security. Electronic banking and electronic commerce depend on large and complex public as well as private networks—so security must be built into every part of the system. The banking industry is focused on the need to defend the integrity of the infrastructure for physical and electronic financial services and is taking the lead to assure that the entire global architecture for financial transactions is safe, secure and sound.

A BITS Tested process, including issuance of a BITS Tested Mark, will be implemented at the Security Lab to evaluate security-related features of products against established criteria. For financial institutions and technology providers alike, the BITS Tested process at the Security Laboratory will provide an unbiased third-party evaluation. The BITS Tested Mark will be given upon successful completion of the testing cycle. Mark issuance will be posted on the BITS Web site.

The BITS testing model is intended to provide an objective evaluation of products against established security criteria. Each financial institution will decide how to apply test results or the lack of testing in product selection decisions for their specific environment. It is reasonable to expect that financial institutions will give favorable consideration to products obtaining the BITS Tested Mark because these products will represent known security features.

The customers of financial services institutions may never become aware of the BITS Tested Mark or the particular product(s) which enhance the security of the online services they enjoy, but the success of the testing process will result in higher standards for product security throughout the marketplace.

### **4. Who is Global Integrity and how are they qualified to do the testing?**

- Global Integrity is a wholly owned subsidiary of Science Applications International Corporation (SAIC). It focuses on the rapidly growing worldwide business of enabling e-commerce through the information protection market. Headquartered in Reston, Va., Global Integrity provides a full complement of information protection, electronic commerce security, consulting and engineering services to global financial institutions and major corporations with electronic operations worldwide. Global Integrity's qualifications are extensive. It currently has the exclusive contract to certify SET (Secure Electronic Transaction) service providers and it manages lab facilities for some of the largest financial services and entertainment industry companies to test proprietary products. Global Integrity and Telcordia are wholly owned subsidiaries of SAIC. Telcordia was one of the key players in developing the ANX standards for the automotive industry and SAIC developed the well-known Common Criteria.

**5. When will the facility be operational? When will the first BITS Tested product(s) be on the market?**

- The facility will be operational at the time of the Grand Opening on July 28, 1999. The BITS Security and Risk Assessment Steering Committee has decided to focus initially on four Product Classes and will have Product Security Profiles developed by November, 1999. The early Product Classes include those that support the Electronic Bill Presentment and Payment (EBPP) area. Issuance of the first BITS Tested Mark will be driven by the specific products selected by technology providers to test and the time required to test the product. We do, however, expect BITS Marks to be issued in 1999.

**6. Who sets the security standards for the products and services tested?**

- The standards are set by the Lab Governance Committee, comprised of security executives at The Financial Services Roundtable member banks, through a development process that has been established. This occurs in conjunction with a collaborative effort among financial services security professionals and technology providers. The testing criteria were developed from various sources such as Common Criteria, OCC Guidelines, ANX Certification Criteria, and more—as well as specific needs of the financial services industry.
- Financial Services Security Lab Criteria Update Meetings will be held at least quarterly to foster a technical interchange and collaborative effort among Security Lab participants. In addition, there will be public peer review of the criteria, since the criteria will be public. Some Lab members will be eligible for membership on the Lab Security Council. This Council is designed to focus on the strategic direction of the Lab as well as to provide direct input into the criteria development process.

**7. How will you coordinate BITS criteria with other existing lab criteria?**

- We are in the process of creating a comparison matrix between the BITS Criteria and the Common Criteria. This comparison may be extended to other criteria as well. The point is to seek consistency around the most effective criteria. To our knowledge, there is no widely recognized security-testing criteria and there is no lab testing criteria approved by an industry-recognized body. BITS and its partners in the Lab have worked with others in the public and private sector to ensure the highest practical security-testing criteria is maintained, and will continue to do so.

**8. What is the timeframe to complete the testing?**

- This is product-dependent. Each product will undergo a pre-analysis phase, in which the testing facility and the technology provider will determine the length of the test.

**9. Will bank or financial services proprietary offerings be tested?**

- Yes, they would go through the same testing process if they offer a product for testing. There will be no differentiation between banks and other technology or service providers that submit a product for testing.

## **10. How will software companies be involved with the BITS Security Lab?**

- Access to the Financial Services Security Lab is open to all interested participants. Membership programs are offered to technology providers based on individual needs. The Lab also offers non-members access to specific services. Software companies and other technology providers may be involved in the Security Lab in several ways:
  - a) Technology providers will have access to the master security criteria and may use this criteria to develop and/or modify product security features.
  - b) A company may bring a product to the Security Lab for a BITS Tested Mark on a member or non-member basis.
  - c) Technology providers may choose to take an active role in the Security Lab Criteria Update Meetings or Lab Security Council.

## **11. How much input would a technology provider have into the criteria process?**

- Security Council members will have a direct role in Product Security Profile development. All Lab members will be able to review and comment on updates to the criteria. Although the Lab Governance Committee will have final say into changes to the criteria, it will strongly consider all input from participating members into the criteria.

## **12. What is the customer expectation for product implementation?**

- Association of the BITS Tested Mark with a product will assure financial institutions that the product meets the published established criteria. On an industry-wide basis, redundancy within the testing process across technology providers will be minimized, leading to a more efficient process, reduced cost and reduced time-to-market.

In some, maybe most, cases, the electronic commerce end-user may not be aware of the BITS Mark or its purpose. However, we do expect that the consumers and providers of eCommerce transaction services will demand increasing levels of security, privacy, and confidentiality.

## **13. What is the initial staff of the BITS Lab?**

- The lab is staffed by Global Integrity's full-time information security professionals. As Product Class testing criteria is completed and demand increases, a documented staffing and equipment ramp-up process will be followed.

## **14. What is the initial investment (start-up costs) and who is paying?**

- BITS and Global Integrity have provided the initial funding, in the multiple millions of dollars. The ongoing model is self-funding by participating members.

# # #