APRIL 2003 / VOLUME 1, NUMBER 10

THE CIP REPORT

FINANCIAL SERVICES ISSUE

CIP PROJECT STAFF

John McCarthy, *Executive Director*

Emily Frye, *Associate Director, Law and Economics Programs*

Kevin "Kip" Thomas, *Associate Director, Research Programs / Research Associate Professor*

Rebecca Luria, *CIP Project Administrator / Executive Assistant*

Dr. John Noftsinger, *Executive Director, JMU Institute for Infrastructure and Information Assurance*

George Baker, *Associate Director, JMU Institute for Infrastructure and Information Assurance*

Ken Newbold, *JMU Outreach Coordinator / JMU CIP Project Liaison*

Contact: cipp01@gmu.edu
703.993.4840

Focus on Financial Services

Few industries have experienced the pace of change that has been witnessed in the vast and diverse activity known as "financial services" over the last decade. Passage of the Gramm-Leach-Bliley Act in 1999 allowed banks, insurance companies and securities firms to affiliate and sell each other's products, which further encouraged a trend of cross-industry mergers and consolidation. A booming economy in the 1990s followed by the burst of the dot-com bubble and the collapse of major corporations raised questions about the standards and practices of the American financial services industry. But perhaps nothing has created change in the industry as much as information technology.

THE TECH CENTER
National Center for Technology & Law
CRITICAL INFRASTRUCTURE PROTECTION PROJECT

Information technology has completely transformed the sector, creating a convergence of products available to customers such as online banking and investment management. IT has created unprecedented efficiencies in this sector and has greatly reduced labor costs. Along with these efficiencies, however, the extensive use of IT in the sector has created vulnerabilities that may be even more attractive to would-be criminals due to the potential for huge monetary gains. Furthermore, the financial services sector is highly dependent on other critical infrastructures such as energy and telecommunications-an outage in one of these sectors could have serious implications for the financial services industry.

Fortunately, this sector recognized these risks many years ago and has worked diligently to address the multitude of vulnerabilities that information technology introduces. As the world witnessed in September 2001, the sector recovered within days of the terrorist attacks, despite the significant concentration of financial services companies in the World Trade Center area. But as is true with every sector, cyber threats will continue to grow in direct correlation with the increasing use of IT.

This issue of The CIP Report focuses on the work of several industry associations to protect this critical infrastructure and introduces our readers to several of the key figures and new issues shaping the financial services sector.

Addressing New Realities

from Congressional Testimony by

Rhonda MacLean, Chairperson

Financial Services Sector Coordinating Council for CIP and Homeland Security

and Senior Vice President, Bank of America Corporation, Corporate Information Security

At all levels across our sector, including executive leadership, operations personnel, our trade associations, professional institutes, and our customers, we are very aware of the new global realities and the importance of the vital financial services we provide globally to the nation and our customers.

The Department of the Treasury recently noted, "We continue to work with the financial and banking communities so that our financial system remains functioning efficiently and effectively. We are confident America's financial infrastructure is strong and resilient." There should be no doubt that the public-private partnership is well engaged to ensure the safety, soundness and resiliency of our industry is not only maintained but also enhanced.

At the time of my appointment, no single entity could legitimately say it represented the financial services sector. Individual associations were actively and effectively working on their members' behalf to provide tools and resources necessary to enhance infrastructure protection. The associations and their members have provided much leadership for our sector and have done outstanding work on various areas, including crisis management efforts, "good practices" knowledge sharing, business continuity practices, and education and awareness initiatives.

Immediately after my appointment in May 2002, we began forming the Financial Services Sector Coordinating Council, with the public sectors' support and encouragement and with the leadership of the Department of the Treasury.

The council consists of the primary organizations that, through their constituencies, represent the majority of the financial services sector. These include key national exchanges, clearing organizations, trade associations in the banking, securities, bond, and insurance segments of our industry and key professional institutes.

Today, 24 organizations are working together to identify and coordinate strategic initiatives that will improve critical infrastructure protection for our sector and with other sectors upon which we depend. The council is a limited liability corporation that has been institutionalized to carry on *(Continued, Page 3)*

Financial Services Sector Coordinating Committee Members

- American Bankers Association
- American Council of Life Insurers
- American Society for Industrial Security
- America's Community Bankers
- Bank Administration Institute
- BITS and The Financial Services Roundtable
- Credit Union National Association
- Consumer Bankers Association
- Fannie Mae
- Financial Services ISAC
- Futures Industry Association
- Independent Community Bankers of America
- Investment Company Institute
- Managed Funds Association
- NASD, Inc.
- NASDAQ Stock Market, Inc.
- National Association of Federal Credit Unions
- National Automated Clearinghouse Association
- Securities Industry Association
- The Bond Market Association
- The Clearing House
- The Options Clearing Corporation

FSSCC *(Continued from Page 2)* the sector's work long after my tenure as sector coordinator is completed. Through our council members, we engage nearly all financial services sector institutions, exchanges and utilities.

At the sector level, this is an example of 'macro' collective leadership being taken to address the new realities. Through this collective leadership and collaboration, we are leveraging the work being performed across the sector for the benefit of the "common good" of our industry. The council model and approach being taken by our sector is being examined by other national critical infrastructure sectors.

This council provides an efficient approach for coordinating the many and diverse participants that comprise our industry sector. Additionally, because there is a corresponding group within the public sector, the Financial and Banking Information Infrastructure Committee (FBIIC), chaired by the Treasury Department, we have the opportunity for direct dialogue on common issues and challenges. The result is an emerging agreement on strategic initiatives we believe will improve infrastructure protection and homeland security.

Five initial strategic areas are the current focus of the council's work. Our approach is to leverage the work already accomplished by our council member organizations to achieve our objectives. Council members are taking primary leadership roles, based on their natural areas of expertise.

The Treasury Department named Rhonda MacLean the Private Sector Coordinator for CIP for the financial services sector in May 2002. Ms. MacLean joined Bank of America in 1996 as Senior Vice President and Director of Corporate Information Security and is responsible for providing global leadership for information security policy, procedures and corporate standards, awareness programs, risk management, and information security technology implementation.

Information Dissemination and Information Sharing - Our goal is to ensure a universal service to disseminate trusted and timely information will be available to all sector participants to increase knowledge about physical and cyber security operational risks faced by the financial services sector. Enhancing the needed services provided by our sector's ISAC is a major focus of our current sector efforts.

Crisis and Response Management - When events occur with broad sector or national impact, a planned and adopted approach for sector-wide crisis management coordination exists, including coordination with government entities. The focus of our efforts is on the ability to communicate and respond as a sector when such events occur.

Sector and Cross sector Outreach - It is important for each organization to determine how to optimally support and commit efforts for achieving the goals of the executive orders and national strategies. We are developing a strategy for sector-wide outreach on homeland security and critical infrastructure protection initiatives that includes regional forums we are conducting jointly with the FBIIC.

Knowledge Sharing - Best Practices - There are numerous "lessons learned" activities and knowledge sharing of "good practices" within various trade associations and among institutions and government entities. We are developing an organized repository to provide this information to authorized institutions and individuals.

National Strategy - We are also leading the sector's effort to revise our sector's "national strategy" document in response to the two national strategies released in February by the President. The *(Continued, Page 18)*

The Financial and Banking Information Infrastructure Committee (FBIIC)

"Working with appropriate members of financial institution regulatory agencies, the FBIIC will coordinate efforts to improve the reliability and security of financial information infrastructure."

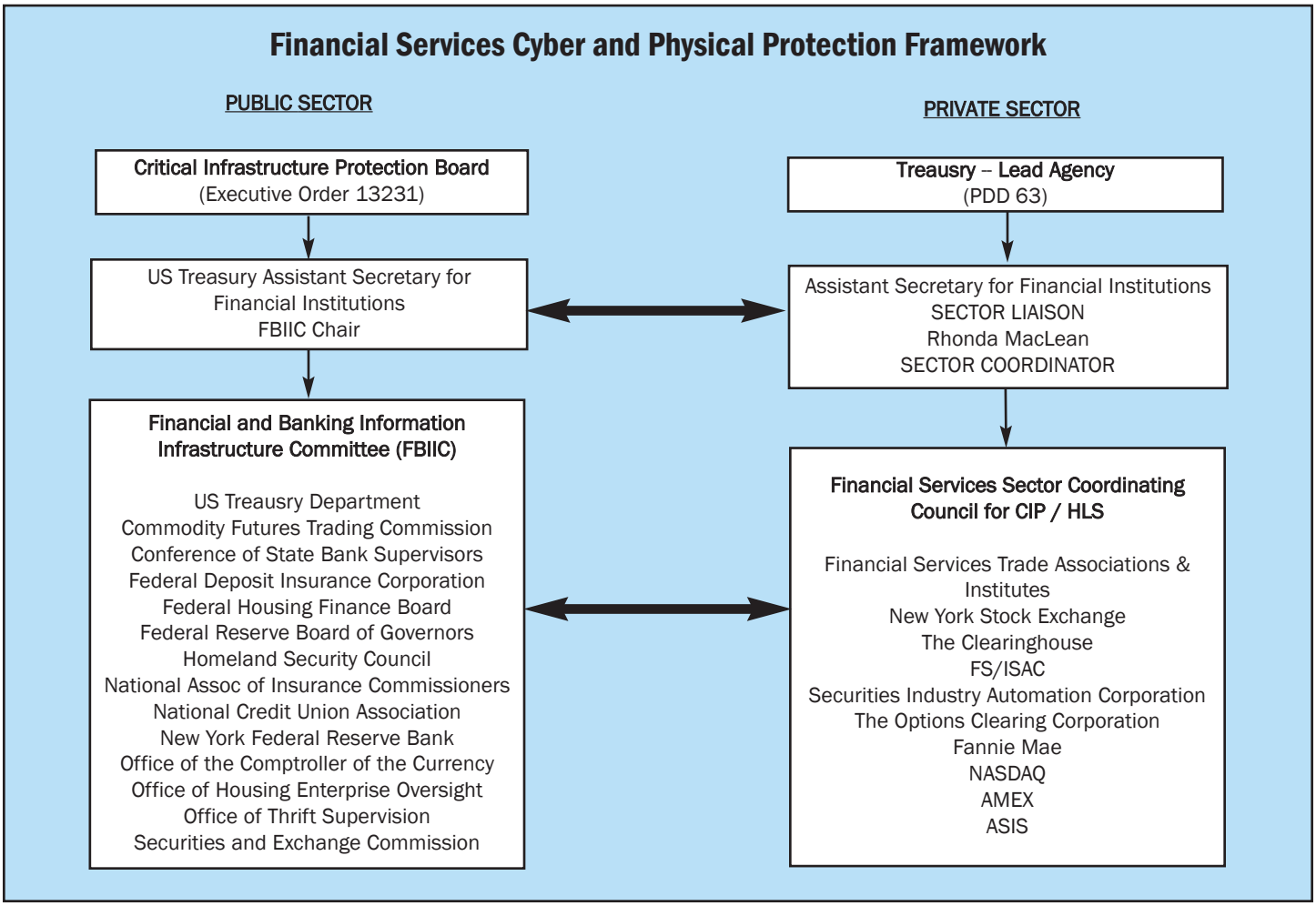
The Financial and Banking Information Infrastructure Committee (FBIIC) is charged with coordinating federal and state financial regulatory efforts to improve the reliability and security of the U.S. financial system. Treasury's Assistant Secretary for Financial Institutions chairs the committee.

In fulfilling its mission, the committee will:

- identify critical infrastructure assets, their locations, potential vulnerabilities, and prioritize their importance to the financial system of the U.S.;
- establish secure communications capability among the financial regulators and protocols for communicating during an emergency; and
- ensure sufficient staff at each member agency with appropriate security clearances to handle classified information and to coordinate in the event of an emergency.

The key objectives of the FBIIC are to identify critical components of the US financial infrastructure, identify vulnerabilities in the infrastructure, remediate vulnerabilities, and evaluate progress.

The FBIIC has five working groups, including the Vulnerability Assessment, Communications, International Affairs, Legislative Affairs, and Telecommunications Service Priority (TSP) Task Group. ❖



BITS Focuses on Key Financial Services Issues

BITS, the Technology Group for The Financial Services Roundtable, was formed by the CEOs of the largest financial services institutions in the United States as the strategic "brain trust" for the financial services industry in the e-commerce, payments and emerging technologies arenas. BITS' activities are driven by the CEOs and their appointees-CTOs, CIOs, Vice Chairmen and Executive Vice Presidents-who make up the BITS Advisory Group and BITS Council. These leaders identify issues, develop strategic recommendations and implement the CEOs' decisions. BITS also facilitates cooperation between the financial services industry and other sectors of the Nation's critical infrastructure, government organizations, technology providers and third-party service providers.

BITS' mandate is to:

- Facilitate the growth of electronic banking and financial services
- Facilitate development of superior, market-driven technologies
- Maintain the industry's role at the heart of the payments system as e-commerce evolves
- Sustain consumer confidence and trust by ensuring the safety, soundness, privacy and security of financial transactions
- Leverage resources and infrastructure across the industry

BITS focuses on those areas that are most pressing to the financial services industry. Current priorities involve issues related to operational risk and are being addressed through BITS' initiatives in Crisis Management Coordination, Fraud Reduction, IT Service Providers, Operational Risk Management, Privacy and Information Use, Security and

Catherine A. Allen
Chief Executive Officer
BITS

Risk Assessment and Payments Strategies. BITS serves an education and monitoring role with its Aggregation Services, Authentication, Patent Issues, and Standards initiatives. Additionally, the BITS Product Certification Program provides the industry with a self-regulatory measure for addressing technology risk. The results range from published business requirements and standards to a communications center for the CEOs in times of crisis.

BITS is governed by a 20-member Board of Directors, Chaired by James E. Rohr, Chairman and CEO of The PNC Financial Services Group.

BITS offers two membership categories: BITS Member Financial Services Organizations and BITS Affiliate Financial Services Consortia and Associations.

The priority initiatives for 2003 were established under the direction of the BITS Executive Committee, BITS Advisory Group, and BITS Council.

Crisis Management Coordination

This initiative focuses on preparation and coordination of member company efforts in a time of crisis, and includes a "call to action" to address issues of interdependencies with other critical infrastructure sectors, such as telecommunications. The scope includes cross-institution and cross industry sector coordination as well as close cooperation with federal, state, and local authorities. The Telecommunications Working Group operates under the auspices of the Crisis Management Coordination Working Group.

Fraud Reduction Program

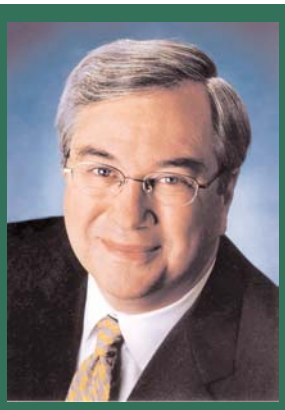
The BITS Fraud Reduction Program provides a coordinated industry means by which to address and reduce fraud through information sharing, standardized reporting, analysis of emerging threats, and cooperative efforts among member institutions as well as key representatives of the vendor community. The BITS Fraud Reduction Steering Committee provides oversight for all program activities. Nine Working Groups address the following topic areas: Collections, Database,

(Continued, Page 6)

BITS *(Continued from Page 5)*
Debit Card, Electronification, Identity Theft, Internet Fraud, Legal, Statistics, and Successful Strategies.

IT Service Providers
This initiative raises awareness, develops voluntary guidelines, and shares successful strategies to assure the security and privacy of services provided by third parties in support of the financial services industry, including those provided through cross border relationships. Effective risk management practices and policies are the foundation of a safe and sound financial services industry. When third parties are involved in providing systems, services, or solutions, financial institutions must establish processes that address risks, vulnerabilities and regulatory requirements at each stage of the service provider relationship. In doing so, the institution must not only evaluate the dynamic areas of risk in the macro-environment, as is the case with political and country risk in cross-border outsourcing, but also the security and privacy controls and vulnerabilities specific to the outsourcing arrangement. The Working Group established an important baseline with the development, in 2001, of the BITS Framework for Managing Technology Risk for Information Technology (IT) Service Provider Relationships.

Operational Risk Management
This initiative focuses on defining terms, providing a forum for information sharing, identifying information security risks, and tracking regulatory changes that could impact financial institutions. BITS formed this Working Group to focus on operational risk issues, given their increased attention and importance to large financial institutions and evolving regulatory requirements. BITS involves the regulatory agencies



James E. Rohr
Chairman and CEO
The PNC Financial Services Group and BITS Chairman

responsible for interpreting and implementing the new Basel II Capital Accord and developing supervisory guidance. The Security Measurement Project Team works with the Security and Risk Assessment Steering Committee to create risk assessment elements for information security. Initial work involves developing a common body of risk factors that influence operational risk and are related to information security.

Payments Strategies
The Payments Strategies initiative focuses on a range of issues tied to legacy and emerging elements of the payments system, including developing analytical tools for use by member institutions, providing educational forums and assessing threats and opportunities. The Payments Strategies initiative is committed to identifying and evaluating the benefits and risks, both strategic and tactical, associated with changes and trends in the payments system. Participants examine the economic impact of the transition from paper-based to electronic payment mechanisms, including the information integrated within these payments mechanisms. The initiative also identifies ways to promote electronic check presentment (ECP) and check safekeeping. Part of its focus is to assess the impact of changes that may result from the proposed Check Truncation Act.

Security and Risk Assessment
This initiative sets priorities to continually bring value to the industry in order to assure the security of the financial services infrastructure, provides information-sharing services, develops voluntary guidelines and business requirements, and provides oversight to initiatives such as those related to IT service providers, product certification against security criteria, and management of operational risk. In recognition of the role of security as a fundamental building block for all aspects of information technology use and e-commerce, the SRA allocates a significant portion of its semi-annual meetings to learning about new risks and risk management tools through educational briefings, presentations, and "roundtable" discussions. In addition, members *(Continued, Page 17)*

LEGAL INSIGHTS

by Emily Frye

What Price Riches? Financial Services Vulnerability in the Age of Anonymous Villains

What does it mean to be the financial leader of the world? Quite simply, it means you're an obvious target. It means that the security and technology you deploy will be watched by those searching for systemic flaws. It means those flaws will be exploited - if not immediately, then inevitably - to the disadvantage of your customers.

Which leaves you with a decision to make: when flaws are exploited, what do you do? From a technology standpoint, the detect-confine-repair methodology seems to have taken effective hold of computer-security departments everywhere. But once the technological solutions have been put in play, the policy issue looms large. When the press discovers that a breach of security has taken place in a consumer-facing financial institution, a feeding frenzy ensues. It is important for financial institutions to plan their strategies in preparation for incidents, and to follow their strategies consistently over time. Doing so will help reduce public panic and media frenzy.

An institution's strategy should have at least two components: a short-term (or immediate) response component, and a medium- to long-range component. The immediate-term response is the most difficult. Financial institutions suffering the effects of cyberattack are faced with a set of all-bad choices:

- Release all known data on the security breach and resulting damage as it becomes available, which makes them look foolhardy, disorganized, and vulnerable;
- Release no data on the security breach and resulting damage, which subjects them to accusations of conspiracy and consumer detriment; or
- Release some data on the security breach and resulting damage, leaving institutions open to the obvious analysis and criticism that Monday-morning quarterbacks - from the press or otherwise - are happy to provide.

The decision as to which strategy to adopt is difficult and unappealing. By linking the immediate-term decision to a longer-term strategy, however, the decision can be rendered more easily.

To use a recent example that received a large amount of publicity, consider the February 2003 hack that resulted in a compromise of approximately 8,000 credit card numbers from some of the nation's most prestigious financial institutions, including Visa, Mastercard, and Discover. The financial industry was criticized for failing to inform consumers, the press, and others about the incident. Yet consider what would have happened if the industry had, in fact, done just that: assume that, as soon as it was aware of a breach, each institution released a statement to the press and immediately contacted all of its consumers who might potentially have been affected. The immediate consequence would have been a flurry of panic at the ever-growing count of the affected, heightened consumer concern, and an increased level of media attention. Since there was no way to know the exact scope of the breach, unaffected consumers might have called in cancellations on their credit cards; they might have stopped using credit cards for some period of time. Both of these measures are costly to the economy and may well have been unnecessary.

Another, more grievous, consequence of immediate disclosure would have been notice to the perpetrators that the financial industry was aware of the problem. To the extent that notice assists criminals in escaping or covering their tracks, immediate disclosure would have damaged the investigative process that is the only opportunity to bring the perpetrators to justice.

As a comparison, consider the effects of a delayed notice. Assume that financial institutions adopted a policy of no immediate notice, but two other forms of

(Continued, Page 8)

Insights *(Cont from Page 7)*
near-term notice:
1. A single deferred and maximally informative notice to affected and potentially affected consumers as early as possible (i.e., once the event has been mitigated, relevant evidence has been secured, and a basic summary can be made); and
2. Cumulative year-end reports to a neutral incident clearinghouse.

This approach, if consistently used throughout the industry, would help consumers feel secure in their relationships with financial institutions. In addition, it would allow managers, regulators, and insurers to make decisions on a solid factual basis.

Tied to a long-term strategy, these measures are even stronger. Both the Financial Services ISAC (Summer 2002) and the Office of the Comptroller of the Currency (APRIL 2003) have released reports indicating that the sector is well along the road toward understanding its major cybersecurity vulnerabilities. It has made solid progress in prioritizing its needs and designing its disaster-mitigation plan.

Plans are good. Moving from plans to preparedness is better - "preparedness" being, unfortunately, a relative and mutable condition. We all know that the target is a moving one. Yet solid progress toward long-term goals is the foundation for trust in short-term measures. Though we do not live in Pangloss' "best of all possible worlds," we can strive for the best in the world of the possible. ❖

Financial Services ISAC Operation Acquired by SAIC

On April 21, 2003 Science Applications International Corporation (SAIC) announced that it signed an agreement to acquire the Information Sharing and Analysis Center (ISAC) and Open Source Intelligence (OSI) business unit from Predictive Systems, Inc. This acquisition will transfer the rights and intellectual property to operate the Financial Services ISAC (FS/ISAC), the Energy/ISAC, the World Wide/ISAC, the Canadian Financial/ISAC, the Japan/ISAC and several Corporate ISACs. The closing of the acquisition is subject to completion of customary conditions, including obtaining consents of customers of the acquired business unit. The closing is expected to occur on or about May 9, 2003.


Suzanne Gorman
FS-ISAC Chairperson

The first ISAC, the FS/ISAC, was created by an SAIC company four years ago in response to Presidential Decision Directive 63. The importance of ISACs was recently reaffirmed by Executive Order, which called for a public/private partnership to share vulnerability and threat information to protect the nation's critical infrastructures. ❖

Regulators Issue Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System

On April 8, 2003 three federal regulatory agencies issued an "Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System." Among other things, the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, and the Securities and Exchange Commission identified sound practices to strengthen the resilience of critical U.S. financial markets and minimize the immediate systemic effects of a wide-scale disruption.

On September 5, 2002, the agencies published for comment a draft of the paper in the Federal Register. The agencies have incorporated many of the suggestions that were made. The final paper, which applies most directly to the clearing and settlement activities of a limited number of financial institutions, provides more flexibility to firms in managing geographic dispersion of backup facilities and staffing arrangements, and takes into account other considerations relevant to cost-effective implementation of sound practices.

The paper can be viewed at http://www.federalreserve.gov/boarddocs/press/bcreg/2003/20030408/attachment.pdf

Secretary Marsh Addresses Security in Madison Day Keynote Address

Ken Newbold, James Madison University

Former Secretary of the Army John O. (Jack) Marsh, Jr. recently delivered the Madison Day address, an annual celebration of the many contributions of James Madison. In his speech, "The Philosopher King", Marsh focused on the debate surrounding "security" versus "liberty" and on how higher education can take a lead in addressing issues in critical infrastructure protection and information security.

In addressing the security and liberty problem, Marsh posed the question, "How much privacy are we willing to give up to have security?" Much of the debate over liberty versus security focuses on privacy rights, but as Marsh states, "If there is no liberty, there can be no right to privacy. For privacy to exist, liberty must flourish." This is a fundamental issue to human freedom, he added. To answer this debate, we must revisit the writings of Madison and bring together participants from government, the private sector, and individual users to "maximize the great advantages of information technology, but minimize encroachments on individual liberties."

According to Marsh, the best place for this conversation to happen is on a university campus; to accomplish this, he says Information Sharing and Analysis Centers (ISACs) should be established on college campuses. Marsh believes the openness and sharing nature of the university culture is the perfect setting for dialogue between various sectors to occur.

Jack Marsh
Former Secretary of the Army

Further, Marsh believes Madison would have met the problems of infrastructure security with a solution that involved a balance between technology and the social sciences. In bringing together experts in policy, law, and technology, the Critical Infrastructure Protection Project has already begun to examine many of the areas that Marsh believes are important to solving the security issues facing our nation. Marsh cited the Critical Infrastructure Protection Project as an excellent example of university collaboration.

Often referred to as the Father of the Constitution, Madison was one of the great political philosophers of his time. He was able to construct the Constitution through his strong understanding of history and philosophy. Madison said, "History can teach us what will or will not work and philosophy can teach us what is right and what is wrong. They are the cornerstones of learning." Binding Madison's beliefs to today's exploding technologies and security issues, Marsh argues it is here, at the core of the liberal arts where the quest for improved security begins.

The week-long annual events commemorating the birthday of James Madison were hosted by JMU's James Madison Center. Transcripts and a recording of Marsh's speech are available at www.jmu.edu/jmuweb/audio_video.shtml. ❖

In January 2003 the GAO released a report, **"Efforts of the Financial Services Sector to Address Cyber Threats."** GAO was asked to review (1) the general nature of the cyber threats faced by the financial services industry; (2) steps the financial services industry has taken to share information on and to address threats, vulnerabilities, and incidents; (3) the relationship between government and private sector efforts to protect the financial services industry's critical infrastructures; and (4) actions financial regulators have taken to address these cyber threats. This report can be viewed at: http://www.gao.gov/new.items/d03173.pdf

ABA Taking Steps to Address Cyber Threats

The American Bankers Association (ABA), an industry group whose membership includes community, savings, regional and money center banks, savings associations, trust companies and diversified financial holding companies, has an active, ongoing program for informing their membership of cyber security issues and providing cyber security resources.

As a member of the Financial Services Sector Coordinating Council, the ABA has taken a lead role in the current education and outreach initiative that is underway at the Council. This initiative is designed to apprise financial sector companies of existing organizations, including the Financial Services Information Sharing and Analysis Center, which can be utilized as a resource for information regarding physical as well as cyber threats and vulnerabilities. A second aspect of the initiative is to garner feedback from financial sector companies as to how the process of sharing such information should evolve, in terms of organization, services, and cost.

In October 2002, the ABA made the "Safeguarding Customer Information Toolbox" available to members to assist them in evaluating their information security and comply with Section 501.B of the Gramm-Leach-Bliley Act of 1999. The toolbox contains resources to assist financial institutions in building their security culture, assessing their information security and risk, managing vendor risk, reviewing their business continuity and recovery efforts, training employees and communicating their information security efforts.

The ABA has also held a series of interactive Webcasts during calendar 2002 and 2003 on a variety of critical infrastructure protection and cybersecurity issues. Additionally, in early 2003, three ABA conferences, the Compliance Conference, the National Conference for Community Bankers, and the Foreword Financial Technology Convention, contain or will contain sessions on information security, as well as technology vendor due diligence and management.

The ABA also distributes a bi-weekly electronic newsletter, the ABA eAlert, which focuses on electronic banking and information security concerns. The ABA website, aba.com, has a series of web pages addressing information security, pointing members to a variety of resources. Other ABA publications, such as the ABA Banking Journal, the ABA Compliance Magazine, and ABA Bankers News have recently contained lead articles regarding critical infrastructure protection and cyber threats.

The ABA was also supportive of the inclusion of computer intrusion reporting under the "Suspicious Activity Reporting" (SAR) obligations contained in 31 CFR 103.18. Under the SAR instructions, financial institutions are now required to file SARs when they suspect someone of gaining access to a computer system of a financial institution to:

- Remove, steal, procure or otherwise affect funds of the institution or the institution's customers;
- Remove, steal, procure or otherwise affect critical information of the institution including customer account information;
- Damage, disable or otherwise affect critical systems of the institution.

Finally, the detection and prevention of identity theft is an area where the ABA has devoted a good deal of attention. For instance, the association has provided members with a

(Continued, Page 12)

Doug Johnson
Senior Policy Analyst
American Bankers Association

Doug's public policy responsibilities include payments system technology and the relationship between technology, privacy, and security. He is responsible for the ABA's recent release of a series of tools to assess information technology risk and safeguard customer information in financial institutions, as well as a resource guide for the identification and verification of accountholders, in response to the U.S. Patriot Act. Doug also works with the FSSCC, BITS, and the FS-ISAC on behalf of the ABA.

THE INFORMATION SECURITY WORK FORCE: The New Millennium

by
Allan Berg, James Madison University

(This is the second installment of a three part series)

Time-based Competition and Product Proliferation Affect the IS Labor Market

Both the pressures of time, and product and service proliferation, play an important role in the market for IS workers. The critical element of time argues for hiring workers who already possess the needed technical skills and experience, who can work productively at once. Otherwise, when faced with a six-month product life cycle, a training period as short as six weeks for a new IS worker or team represents one quarter of time-to-market. In that scenario, an employer risks missing the market window altogether and, thus, the stream of revenues needed to keep the company in this environment, in high-tech competition. Similarly, an extended breaking-in period for an employee increases the chance that a customer's project deadline will not be met. Product proliferation creates the need for IS workers specialized in particular technical skills and their application. Taken together, time and product proliferation produce the demand for "the right worker, with the right skills, at the right time." But can the "producers" of skilled IS worker's match to corporate pace?

The Niche IS Labor Markets

The mix of knowledge and skills required can vary significantly from one IS job to another, in terms of the specific technical skills needed, industry knowledge and experience, and other qualifications in areas such as project management, communications, organizational and legal skills. Thus IS workers qualified for one job may not qualify for another. Certain technical skills may be in high demand or "hot," or be new skills such as e-commerce specialists-with employers having difficulty recruiting and retaining people with those skills. Also, IT is changing rapidly, which causes companies to frequently need different skill sets in the IS worker.

The Make vs. the Buy Decision

As time has become an increasingly important factor of competitiveness for many employers of IT and IS workers, the time available to retrain existing employees or train new employees in the skills needed for new projects has diminished. Companies are forced by short product life and short product development cycles to hire new employees or reassign existing workers in ways that do not require a lot of break-in training before they can be productive.

In this environment, many companies have concluded that they cannot afford the time penalty and the uncertainty associated with "making" the employees they need (through training or retraining). Many employers are, instead, pursuing a "buy" strategy, seeking the exact skills and experience they need in an IS worker and paying a premium for that. Or, as reported by the Gartner Group, "the pace of technological change is making the outside IS market the best source and repository of intensive technology skills."

There is, of course, a time risk associated with seeking to recruit and hire the candidate with the exact skills and experience, especially in a tight labor market. Outside hires also lack important, company-specific knowledge, and may be less committed and loyal to the employer.

Companies also pursue buy decisions for other reasons. First, in fast-growth IT companies, often every core IT and IS worker is deployed on current projects leaving none available for retraining. Second, in a dynamic, fast paced, highly competitive environment such as IT and IS, the technology paths are often uncertain, making it very difficult to project future skill needs.

Though the "buy" strategy generally requires paying a premium for the requisite skills, companies

(Continued, Page 12)

Work Force *(Cont from page 11)* are able to reduce the risks associated with the uncertainty about their future skill needs, while reducing or even eliminating the cost of training. At the same time, employers can be reasonably assured that new hires are able to hit the ground running.

Disincentives to Train the IS Worker

The current IT business environment and its effect on the highly-skilled IS labor market increase the risk of training investments and reduce the likelihood of capturing an acceptable return on the investment.

The tight IT labor market-a function of both the rapid demand for core IS workers, generally, and the need to fill specific niches-has created an environment in which many companies seek to find the people they need by luring talented IS workers away from their current employers using a variety of mechanisms. These inducements (in the form of compensation, benefits, and better quality of working life conditions) encourage job-hopping among IS employees, creating another major disincentive for companies to train or retrain IS workers. Companies that invest in the training of employees to upgrade their IS skills may create an attractive target for poaching by other companies, putting at risk both the employees and the companies' training investment.

Recruitment and Retention

The business environment in IS has created a labor market in which job hopping serves as a means to gain the vital technical skills needed for career opportunities. IS jobs are now regarded as another element of the training process, of learning by doing, and employees move from job to job to gain new skill sets and experiences rather than assume they will stay with a particular company for life. Acquiring new skills allows them to move within the entire IS work community for opportunities, rather than solely within a particular company.

IS workers tend to see "challenge and responsibility" and "job atmosphere" ahead of "salary" as what matters the most to them about their jobs. Having quality of working life issues, job stability, and the opportunity to gain critical skills through job assignments lead over all other factors.

Recruitment of IS Workers

Not all employers of IS workers enjoy a well-oiled and nimble human resources department, with sophisticated and creative recruitment methods, and a streamlined hiring process. Many small companies do not have human resource departments at all; and, technical professionals who have little or no knowledge and experience in human resources practices may perform hiring functions. Many companies contract with recruiting firms to fill their jobs, but many of these recruiters lack the technical knowledge to do much more than follow the technical specification the hiring firm provides. Making the labor markets work better-in terms of effectively identifying the critically needed IS skills, rapid identification of potential candidates, and streamlining the internal hiring process-could help reduce the time it takes to staff operations and reduce vacancy rates. ❖

ABA *(Continued from Page 10)* Communications Kit that is designed to help bankers provide their customers with the resources and information they need to protect their identity. The association, as part of its "Financial Privacy Toolbox," also made training aids available to assist front-line bank personnel in spotting pretext calling, a technique commonly used by identity thieves.

The ABA, in conjunction with LexisNexis, has also recently released InstantID, a service that verifies customer account information across multiple databases, validating that such information as name, address, date of birth and social security number are authentic and identifying potentially high-risk data elements, for example, miss-matched addresses, prison or campground addresses, disconnected phone numbers, or Social Security numbers of deceased persons. In addition to helping reduce fraud and identity theft and complementing existing fraud tools, IDPoint can also play a valuable role in assisting the bank fulfill the new account opening requirements in the USA PATRIOT Act. ❖

"Straight-Through-Processing" in the Clearance and Settlement of Securities

In July of 2002 the Securities Industry Association's board of directors unanimously approved a straight-through processing program for the clearance and settlement of equities, bonds, and other securities.

"The overall goal of SIA's earlier STP/T+1 program to convert from T+3 to T+1 settlement by 2005 has been replaced by a set of challenging, straight-through processing goals to be accomplished over the next two years," said Allen Morgan, Jr., chairman of SIA's board and chairman and CEO of Morgan Keegan & Company. "This will result in significant benefits to firms and investors."

Straight-through processing (STP) is best described as the seamless integration of systems and processes to automate the trade process from end-to-end-trade execution, confirmation, and settlement without manual intervention or data entry. T+3 means that purchases and sales must settle three days after the transaction has occurred, the current industry standard for corporate securities.

"The industry needs to focus on more effective straight-through processing before it is in a position to fully evaluate a conversion from T+3 to T+1 settlement," Morgan said. "We believe that the settlement period should be evaluated again in 2004."

The board-approved STP program will build on SIA's STP/T+1 program, which has been under way for the past three years. The new program will focus on STP in 2003 and 2004, rather than on shortening the settlement cycle to T+1 in 2005. Key projects include: improved processing of institutional trades; electronic book entry to replace physical securities and payments; and, a range of other automation projects which address the processing of corporate actions (such as recapitalizations and dividends), stock lending, syndicate underwriting, and other operations functions. "The work of hundreds of industry volunteers on the STP/T+1 program over the last three years has provided a solid platform and clear direction for industry STP priorities in 2003 and 2004," said Marc E. Lackritz, SIA's president. "The board's decision to focus attention on STP reflects the industry's continuing commitment to investing in new clearance and settlement technology."

Donald D. Kittell
Executive Vice President
Securities Industry Association

"SIA is committed to working with the Depository Trust & Clearing Corporation and other industry clearance and settlement organizations, the Bond Market Association, securities firms, custodian banks, institutional asset managers, retail investors, securities issuers, and industry regulators to improve the performance and productivity of the clearance and settlement system," said Jeffrey Bernstein, chair of the SIA STP Steering Committee.

"There are challenges ahead, but, as has been the case with the transition to the year 2000, the conversion to decimals, and the opening of the markets following September 11, there are many dedicated industry volunteers whose expertise will enable us to move smoothly to straight-through processing," Bernstein said. ❖

Open-Source Software, Proprietary Software: Implications for National and Economic Security

By Emily Frye

Open-source software has received increasing attention in recent years. Academic journalists, businesspeople, and lawyers find open-source software a matter of concern for several reasons. First, it offers a fundamentally different model for software development from that to which we are accustomed: it exposes code to development and critique from both paid and unpaid, known and unknown parties. Second, its revenue potential is often unclear. Why would someone choose to write code for which they will not receive compensation? In a market-driven economy, it can be difficult to understand non-monetary motives.

In January 2003, the CIP Project undertook a study of the potential implications of open-source software on national and economic security. The open-source study, led by Albert Tramposch (Co-Director of the George Mason University School of Law's Intellectual Property program), expects to identify the major questions that need to be answered in order to formulate a sound public policy with regard to open-source software. Legal and policy developments that occur prior to the completion of the study will be factored into the end product. The results will be published as a paper for wide distribution to the legal, policy and technology community.

The study appears to have hit a nerve: without any outreach efforts, the study team already has been asked to

- peer-review work on open-source software that is being prepared for the International Telecommunications Union (ITU);

Emily Frye is Associate Director of Legal Programs for the CIP Project

- prepare a proposal to present its findings at the 2004 meeting of the American Bar Association; and
- document its findings for the January 2004 issue of the IEEE magazine focused on open-source issues.

One important element of the study brought together leading proponents of diverse views for a day of explication and debate. On March 28, over 80 software professionals and business executives gathered at the George Mason University School of Law to set forth their views on open-source software, the economy, and national security. The conference was an outstanding event, and its success was due in large part to the coalition-building approach taken by the study team. One of the team's strengths is that it seeks to understand, instead of polarize, the true range of opinions (and reasons for opinions) on the issues surrounding open-source software.

The basic questions that the team is exploring are identified below.

Economic Security

The U.S. software market has built its strength based upon a proprietary development model that achieves revenue through licensing individual copies of software to large numbers of customers. The open-source model of development is different. Some software that is developed in the open environment can be licensed for profit, and some can not, depending upon the licensing structure that its developers adopt. If the software can not be licensed for profit, is there any way to sustain an economic development model for this type of software? Can revenue from maintenance, customization, user training or other services supply enough income to keep the U.S. software economy strong?

National Security

In the traditional software

(Continued, Page 15)

O-S *(Continued from Page 14)*
economy, customers are expected to use software that is provided to them in "compiled" format, and are not expected to, or able to, review the code itself. In the open environment, by contrast, users are often seen as knowledgeable contributors to the code itself. The code is available to them for review, inspection, and even change. In a broad-based open development environment, a very large number of eyes is reviewing and developing the code. While proprietary development entities can conduct background checks on their developers, open-environment developers do not examine one another's history. Is it more likely that malicious code will be inserted into broadly deployed software or, of more concern, into software that is used by the defense industry for national security purposes? This is of particular concern because free downloads of open-source software may take place on defense-operated (or other sensitive) systems without legal or other review - since the software isn't being licensed for a fee, the typical approval process can be easily circumvented. The installation of free, but potentially vulnerable, software, has raised the spectre of widespread, untracked introduction of vulnerabilities. To what extent does the many-eyes theory enhance software security; to what extent does it reduce software security? Furthermore, if an unfriendly government becomes aware that the U.S. government uses an open-source product, might it assign experts to review the product code to exploit any weaknesses?

For more information on the open-source study, contact Emily Frye, Associate Director of Legal Programs at the CIP Project, at 703-993-4170 or ffrye@gmu.edu ❖

Critical Infrastructure Protection: Legal Questions at the Forefront of National Security

A conference sponsored by the CIP Project of the National Center for Technology and Law, GMU School of Law

May 9, 2003

This one-day conference will feature leading academics and practitioners seeking answers to the following questions:

- Terrorism and Tribunals: What is the proper forum for prosecuting terrorists?
- Cybersecurity and Self-Help: Do UCITA and the Berman Bill create a precedent in law that harms or helps Critical Infrastructure Protection, and what self-help regime would be socially optimal for protecting critical infrastructures?
- Limits on Government Responses to Terrorism: What are the roles of the First Amendment, posse comitatus, and the right of privacy in circumscribing government action to quell terrorism?

Former Virginia Governor Jim Gilmore will give the luncheon keynote on "Homeland Security and the Right of Privacy."

Participants include Amitai Etzioni (The Limits of Privacy); Maj. Gen. John Altenburg (former Deputy Judge Advocate General of the U.S. Army); David Rivkin (former White House counsel); Lawrence Greenberg (General Counsel of the Motley Fool), and many other exciting and provocative figures.

There is no fee, but an RSVP is required.
For more information on the conference, contact Emily Frye at ffrye@gmu.edu or (703) 993-4170.

UK Treasury Issues Report on Emergency Authority for "Major Operational Disruptions"

By Lee Zeichner, Esq.

Financial authorities in the UK have issued a report on managing crisis similar in scope to the 9/11 attacks. HM Treasury in the UK (UK Treasury) prepared the report, titled Financial Systems and Major Operational Disruption, in an effort to gather comments and insights from industry stakeholders. The UK Treasury is responsible for formulating and putting into effect the UK Government's financial and economic policy. The report concentrates on alternative strategies for coping "with the effects of a major operational disruption." UK authorities define disruptions to include not only terrorist attacks, but also significant IT failures and natural disasters that result in catastrophic damage to critical financial services and functions.

The UK financial service authorities are still grappling with ways to manage large-scale terrorist attacks that undermine financial activity. Whether coincidental or not, UK authorities have proposed strategies similar to those implemented by US supervisory agencies and regulators. These include a focus on wholesale services (payments, clearance, settlement), improving recoverability, enhancing operational resilience, understanding infrastructure interdependencies - especially telecommunications, and considering new emergency and crisis activity. In the UK, three separate entities manage sector activities, including the UK Treasury, the Bank of England and the Financial Services Authority (FSA). The UK Treasury closed the public comment period late last week.

The report assesses five areas of focus:

- Current approaches: Current legal and business practices for managing operational crisis in the UK are not sufficiently robust. Practices include market-based negotiations, contracts, and cross-sector collaborative efforts. The UK Treasury suggests that market-based tools are preferred for dealing with disruptions, but that existing collaborative mechanisms are insufficient given the harm that could result.

- Legislation: The UK Treasury is considering legislation to supplement current approaches. Additional authorities would promote order by (1) providing "breathing space" to identify and address operational problems and (2) in some "exceptional" cases, intervening (e.g., to close markets and systems). The UK Treasury clearly prefers to leave crisis management to industry, excluding intervention by the UK government in purely financial crises or where industry does not support the UK government's intervention. In contrast with discussions in the US, the UK Treasury's proposals emphasize this preference for minimalist governmental intervention.

- Evolving framework: The UK Treasury considers how, and the extent to which, new authorities would be implemented. The UK Treasury recognizes the global nature of financial services and questions how emergency powers would be applied for non-UK entities. The UK government is also thinking through administrative rules for crisis management.

- Suspension of obligations: Suspending obligations is one of the more complex areas examined in the report. The purpose of obligation suspension would be to "create breathing space" during or in the aftermath of a major disruption. Specifically, the UK government is considering how suspension powers might be used and whether they would be beneficial. The report hypothesizes several complex examples, including a firm's failure to make payment on a derivatives contract after a terrorist attack. Suspension would freeze market positions and obligations. The UK government is especially interested in crafting rules that respect market relationships but also protect critical wholesale functions. The report seeks comment additionally on the extent to which

(Continued, Page 17)

UK Treas *(Cont from Page 16)*
these same powers should be created for retail transactions.

● Direction of infrastructure: The final section of the report examines strategies for the UK government to collaborate with high-volume service providers and segments of the financial services sector in the UK. These would include financial utilities, "recognized" exchanges and clearing houses (similar to self-regulating organizations in the US), and investment exchanges - deemed financial infrastructure in the report. These strategies raise some of the more knotty issues associated with balancing market principles with the best interests of the public.

UK officials raise the following seven questions that must be addressed in the coming months to enhance resiliency of financial infrastructure in the UK:

Key Questions

1. Is there more that could usefully be done by the private sector to strengthen the contingency provisions in contracts and other legal instruments?
2. Is there a role for the authorities in assisting with this?
3. Is there more that could usefully be done by the private sector to strengthen market cooperation? Is there a role for the authorities in assisting with this?
4. In principle, would it be useful to have new legislation to help promote order in the financial system in the face of major operational disruption?
5. Have you any comments on: how new legislation might address risks; the possible disadvantages and limitations of new legislation; and general constraints on new legislation?
6. If new legislation were to be sought, are the suspension and direct powers the right choices? Are there any other types of legislation that might be useful to promote order in the financial system?
7. Do you support the idea of a suspension power? Do you support the idea of a direction power? ❖

BITS FINANCIAL SERVICES ROUNDTABLE

(Continued from Page 6)
of the group participate in outreach activities with associations, industry consortia and universities that focus on information security issues. The Security and Risk Assessment Executive Committee sets the direction for the SRA Working Groups and oversees and contributes to all of BITS' security related initiatives.

Privacy and Information Use
This initiative provides a forum for BITS members to exchange information on a range of topics involved with use of consumer information for business purposes; tracks and works to influence the development of standards and specifications for technologies used to enable consumers' privacy preferences such as P3P; and conducts primary research about effects on consumers' financial services behaviors from concerns about privacy and security. Use of information about consumers is fundamental to financial institution business models.

Additional BITS initiatives are either being completed in 2003 or are maintained on a limited basis.

Aggregation Services focuses on achieving consensus on voluntary guidelines for sound business practices to ensure security and privacy in online aggregation services.

Authentication addresses a range of issues related to identity management and authentication of entities involved in e-commerce, from assessing the competitive landscape to identifying successful strategies.

Patent Issues provides educational services, monitors patent issues, and works directly with the US Patent and Trademark Office to improve the speed and quality of the patent process as it affects BITS and FSR member financial institutions.

Standards monitors the standards-setting environment to determine when, and where, standards are being developed that impact the financial services industry. The group offers recommendations when direct industry participation is warranted.

Please visit the BITS website, www.bitsinfo.org. ❖

FSSCC *(Continued from Page 3)* strategies are focused on "The Physical Protection of Critical Infrastructures and Key Assets" and "Securing Cyberspace." This is our opportunity to define strategic as well as tactical, actionable and measurable programming, to direct and advance our sector-wide critical infrastructure and homeland security efforts and to address the recommendations outlined in the national documents strategy referenced above.

In my chairperson role for the FSSCC, I work closely with our lead agency, the Department of Treasury, and the Financial and Banking Information Infrastructure Committee (FBIIC), to ensure our mutual goals are addressed to the benefit of the economy and to all financial services customers. It is through council members' cooperative efforts, their member institutions, and the strong leadership provided by the Treasury and through FBIIC, that we are able to maximize our resources and achieve our objectives to ensure protection of our critical infrastructures to the benefit of the economy and to the public. ❖

The CIP Project is part of the National Center for Technology and Law at the George Mason University School of Law. It is a joint initiative between GMU and JMU that examines law, technology, and policy to find comprehensive solutions to the most pressing CIP issues for policy makers and critical infrastructure owners and operators. The CIP Project was launched in May 2002. The CIP Project encourages participation by representatives from all levels of government, academia, and private industry.

The CIP Report is published by LegalNet Works, Inc. on behalf of the CIP Project. Formed in 1996, LegalNet Works Incorporated focuses on the development of information security laws and regulations with an emphasis on liability, risk management, national security, regulatory compliance, and privacy. LegalNet consults both government and industry officials on legal and policy reform in these complex areas.

If you would like to be added to the distribution list for The CIP Report, please send an e-mail to cipp01@gmu.edu.