"Closing the Gap"

A Research and Development Agenda to Improve the Resiliency of the Financial and Banking Sector

U.S. Department of Treasury - Office of Critical Infrastructure Protection and Compliance Policy

Financial and Banking Information Infrastructure Committee

Financial Services Sector Coordinating Council

Contents:

For more information, contact:

- D. Scott Parsons, Deputy Assistant Secretary Office of Critical Infrastructure Protection and Compliance Policy (scott.parsons@do.treas.gov)
- Brian Peretti, Program Manager, Office of Critical Infrastructure Protection and Compliance Policy (brian.peretti@do.treas.gov)
- Dr. Jerrold M. Grochow, Consultant, MITRE Corporation; Vice President for Information Services & Technology, MIT (jgrochow@mit.edu)

Introduction

The continuous operation of the financial and banking system in the United States is key to all organized economic activity. Protecting the financial and banking infrastructure has been recognized as a national priority and has been receiving increased attention in organizations connected with this sector. In the past several years, many of these organizations have significantly improved their awareness of vulnerabilities and their ability to respond to threats

and attacks. Most would agree, however, that there is much to be done in achieving a national financial and banking infrastructure that is both highly resistant to attack, both physical and "cyber", and also highly resilient in the event that an attack does occur.

The Treasury's Office of Critical Infrastructure Protection and Compliance Policy (CIP&CP) has been working with public and private sector institutions in the financial and banking sector to assess vulnerabilities and highlight areas for improvement. As part of this effort, CIP&CP has created a research and development agenda (R&D Agenda) aimed at improving both the state-of-the-art in Critical Infrastructure Protection (CIP) as well as the state-of-the-practice as it relates to this sector of the economy. General research topics as well as specific projects have been identified that, if accomplished and the results implemented, will improve both the technologies and business practices related to CIP. The Agenda's overall goal is to support research and development activities and process improvements that will raise the overall level of the sector's preparedness and resiliency as well as the individual level at each institution. Projects oriented to "closing the gap" between available state-of-the-art technologies and business practices and those that are actually implemented (the "state-of-the-practice") are a particular priority.

As CIP became a topic of national (and international) interest, governmental and non-profit organizations began to assess the state-of-the-art and highlight those areas that required further R&D. Most of these efforts were oriented to technology R&D, rather than business practice R&D, and did not particularly highlight the needs of any one sector of the economy. CIP&CP reviewed the output of these activities (see the Source Material list) and other documents and met with various industry experts. These meetings led to the creation of an R&D Agenda to address the needs of the financial and banking sector. The reader will find that most research areas on the CIP&CP list are, therefore, familiar (with sources identified), although the focus and detail has been related to their value to the financial and banking. Many of these projects will have value across other sectors as well.

The R&D Agenda's suggested projects come from many sources. They have been classified according to several different criteria to ensure that the totality will span all facets of the "CIP life-cycle," a wide variety of technology and business practice areas, short- to long-term development timeframes, as well as low- to high-risk in terms of achieving useful outcome.

As a result of our methodology, research by government, private sector, or public sector institutions may be being conducted on topics that are the same or similar to the ones listed in the R&D Agenda. As the R&D Agenda emphasizes the interests of the financial and banking sector, "high priority" projects have been gleaned from the general list. Topics have been listed as "high priority" if they represent R&D areas that are not only of significant interest to the financial and banking community, but also are uniquely addressed under the mission of the CIP&CP Office. It is expected that R&D awards under this program will span a majority of the various classifications with emphasis on "closing the gap."

Several factors contribute to the inability to "close the gap" between the state-of-the-art and the state-of-the-practice in CIP. First, what we "know should be done" is often at a high level ("networks must be more secure") rather than at a detailed operational level ("implement this protocol and this business practice in this way"). Second, improving an organization's CIP state-

of-the-practice requires resources that may other have competing demands, and whose business case may not always clear. Lastly, in some areas we do not know how to make enterprises both highly impervious to attack while also making it able to quickly recover if its defenses are breached. As a result, there is much to do in expanding the state-of-the-art. Research is encouraged in all aspects of developing solutions to these problems for the financial sector.

Relevant Presidential Directives and Action Recommendations:
From Presidential Decision Directive 63 (May 1998): "Department of the Treasury and the financial sector are expected to:

- Assess the vulnerabilities of financial and banking to cyber attacks and recommend measures to eliminate significant vulnerabilities;
- Develop an Industry-owned and operated information sharing system for identifying and defending against major cyber attacks;
- Recommend a program of research and development to keep the industry at the cutting edge of information systems security; and
- Develop and implement an industry-wide information system vulnerability awareness and education program."

From the National Strategy to Secure Cyberspace: **"A/R 3-6:** A public-private partnership should continue work in helping to secure the Nation's cyber infrastructure through participation in, as appropriate and feasible, a technology and R&D gap analysis to provide input into the federal cybersecurity research agenda, coordination on the conduct of associated research, and the development and dissemination of best practices for cybersecurity." "**A/R 2-12:** To optimize research efforts relative to those of the private sector, DHS will ensure that adequate mechanisms exist for coordination of research and development among academia, industry and government, and will develop new mechanisms where needed."

Research topics were selected based on the following criteria:

- CIP research of interest to the financial and banking sector.
- Generally does not include topics of broad general interest (e.g. software development methodologies, secure hardware).
- May include topics of interest to other industry sectors, but impact focuses on finance and banking.
- R&D may include the creation of "best practices" and ways of improving the "state-of-the-practice" as well as the "state-of-the-art."

Program Areas – CIP "life-cycle" (extension of framework in "Finance and Banking Sector, The National Strategy for Critical Infrastructure Assurance"):

- Policy and Strategy
- Awareness and Assessment (and Understanding/Training)
- Preparation and Prevention (Protection and Deterrence)
- Detection and Reaction (Response)
- Recovery and Restoration (Decontamination and Reconstitution)
- Risk Management (Financial and other)

Research Impact/Impact Areas – business practice or technology characteristic:

- Business continuity, system backup and recovery (BusCont)

- Information security and privacy, including encryption technologies (InfoSec)
    - anti-virus, PKI, vulnerability assessment, content scanning, application security, and various encryption technologies.
- Authentication and access control (A&AC)
    - Internet access control, intrusion detection, security appliances, firewalls
- Network, communications, and messaging protocols (NetProt)
    - virtual private networks (VPN), common message protocols, XML
- Operations center management (OpCtr)
- Third party relationships, outsourcing, etc. (3rdParty)
- Interdependence with other areas, e.g. telecommunications (Interdep)
- Best practices (BP)

Timeframe:

- Expected timeframe for research to produce commercially viable results. Industry adoption timeframe begins when commercially viable results are available and may be significant.
- Near-term is 12-24 months.
- Mid-term is 2-4 years.
- Long-term is greater than four years.

Research Risk:

- Each research area is rated as to "risk" of achieving a commercially useful outcome in the desired timeframe.
- Distinguishes between "developmental" activities (low risk) vs. areas where the expected outcome has a higher degree of uncertainty or may not even be known when the research is begun (high risk).
- Technology development risk is based on whether a research area is extending technologies already in wide-spread use as well as whether significant breakthroughs are required to achieve desired results.
- Risks associated with implementing new or better business policies and processes are related to the likelihood of achieving adoption and benefits.

Source:

- Documents, including public and private research studies, government documents, articles, white papers, etc. used as source materials.

Priority:

- Priority specifically (1) for improving the resiliency of the finance and banking sector, AND (2) for the purposes of funding this R&D Agenda. Priorities are thus related to BOTH the finance and banking sector, and to the specific R&D program that should be managed by the Treasury CIP-CP office.
- Based on impact, risk, cost, uniqueness, time frame, and other factors relevant to the specific research item.
- Other projects may be high priority for improving the resiliency of the finance and banking sector, but are already being addressed by other government granting or research programs.

Estimated Funding:

- "Order of magnitude" estimates of funding required for initiation of an effective R&D program.
- Total expected funding to achieve implemental results would be determined during the initial project stages.

Description:

- Short description of the example R&D project.
- Intended to give a general framework for the R&D area.
- Provides general guidance rather than specifying detailed requirements.

Summary of High Priority Topics for Funding via Treasury CIP-CP Initiative

Research Topic (not in priority order)	***Program Area***	***First Commercial Use Time-Frame***	***Research Risk***	***Funding Estimate*****
Best practices repository	Preparation and Prevention	Near-term	Low	Less than $1M
Standards for end-to-end testing of industry backup systems	Policy and Strategy; Risk Management	Near-term	Low	Less than $1M
Life-cycle costing	Risk Management	Near-term	Low	Less than $1M
Implications of industry outsourcing	Policy and Strategy; Risk Management	Near-term	Low	Less than $1M
Security procedures to defend against "insider" cyber-attacks	Awareness and Assessment, Preparation and Prevention, Detection and Reaction	Near-term	Low	$1-3M
Business continuity strategies	Policy and Strategy, Recovery and Restoration	Near-term	Low	$1-3M
Data replication best practices	Recovery and Restoration	Near-term	Low	$1-3M
Clearing systems interoperability	Preparation and Prevention, Recovery and Restoration	Near-term	Low	$1-3M
Patch clearinghouse	Preparation and Prevention	Near-term	Low	$1-3M
Creating public policy to promote improved critical infrastructure protection	Policy and Strategy	Near-term	Medium	Less than $1M
Asset movement pattern recognition	Detection and Reaction	Near-term	Medium	$3-7M

Research Topic (not in priority order)	***Program Area***	***First Commercial Use Time-Frame***	***Research Risk***	***Funding Estimate*****
Data replication technology	Preparation and Prevention, Recovery and Restoration	Near-term	Medium	$3-7M
Enterprise security management	Policy and Strategy, Awareness and Assessment, Preparation and Prevention	Mid-term	Low	$1-3M
Wide-spread identity theft	Preparation and Prevention; Detection and Discovery; Recovery and Restoration	Mid-term	Medium	$1-3M
Technology to defend against "insider" cyber-attacks	Awareness and Assessment, Preparation and Prevention, Detection and Reaction	Mid-term	Medium	$3-7M
High reliability biometric identification systems	Preparation and Prevention	Mid-term	Medium	Greater than $7M
Securing software environments including commercial "off-the-shelf" software	Preparation and Prevention, Detection and Reaction	Mid-term	High	Greater than $7M

Example R&D Agenda Topics

#	Research Topic*	Program Areas	Impact (Impact Area)	First Commercial Use Timeframe	Research Risk
1	*Enterprise security management*	Policy and Strategy, Awareness and Assessment, Preparation and Prevention	Increased control over security for the entire enterprise (BP)	Mid-term	Low
Source: I3P Cyber Security R&D Agenda; NRC Making the Nation Safe				Funding Est.: $1-3M	Priority: HIGH
Description: "Integrating diverse security technologies into a coherent capability for maintaining access to and use of enterprise resources, monitoring behavior on enterprise systems, and detecting and responding to suspicious or unacceptable behavior… Research in the areas of enterprise policy definition and management, definition and maintenance of a targeted risk posture, and definition of, and protection at, security boundaries." [I3P] "Develop better system-administration tools for specifying security policies and checking against pre-specified system configurations…Create and employ metrics to determine the improvement to system security resulting from the installation of a security measure." [NRC]					

#	Research Topic*	Program Areas	Impact (Impact Area)	First Commercial Use Timeframe	Research Risk
2	*Integration of physical and cyber security*	Policy and Strategy, Awareness and Assessment, Preparation and Prevention	Increased control over security for the entire enterprise (BP)	Mid-term	Medium
Source: http://www.opensecurityexchange.com					
Description: IT attacks can amplify the impact of physical attacks and vice versa. "The lack of technical integration between physical and IT security systems has resulted in organizational and procedural gaps… [organizations are] unable to consistently implement security policies."					

#	Research Topic*	Program Areas	Impact (Impact Area)	First Commercial Use Timeframe	Research Risk
3	*Network security standards coordination*	Preparation and Prevention, Detection and Reaction	Decreased vulnerability across heterogeneous connected networks (InfoSec, NetProt)	Mid-term	Medium
Source: I3P Banking and Finance Sector Workshop, June 24-25, 2002; NRC Making the Nation Safe					
Description: Research focusing on improving coordination of security standards across network connections, ensuring security across wired and wireless devices, with particular concern being given to both for interoperability and privacy.					

#	Research Topic*	Program Areas	Impact (Impact Area)	First Commercial Use Timeframe	Research Risk
4	*Secure software development methods*	Preparation and Prevention, Detection and Reaction	Provide more secure systems (InfoSec)	Mid – Long-term	High
Source: I3P Survey of R&D; NRC Making the Nation Safe					
"The approach taken to information infrastructure protection (I2P) in software engineering methodologies practiced today is inadequate to support the goals of full integrated end-to-end security in new systems. Research is needed to establish more robust security practices in code development and to determine how these practices can be made general." [I3P]					

#	Research Topic*	Program Areas	Impact (Impact Area)	First Commercial Use Timeframe	Research Risk
5	*Securing software environments including commercial "off-the-shelf" software*	Preparation and Prevention, Detection and Reaction	Improved security of integrated computer system environments (InfoSec)	Mid-term	High
Source: National Scale INFOSEC Research Hard Problems List				Funding Est.: greater than $7M	Priority: HIGH
Description: Almost all financial and banking institutions are dependent on at least some commercial off-the-shelf (COTS) software, whether for accounting, Customer Resource Management (CRM), or mission specific functions. Current security technology does not provide appropriate solutions in an environment integrating COTS packages. Methods are needed for integrating COTS components (as well as custom developed software) from multiple vendors into secure computer environments that also give consideration to usability of the security mechanisms.					

#	Research Topic*	Program Areas	Impact (Impact Area)	First Commercial Use Timeframe	Research Risk
6	*Access control language standards*	Preparation and Prevention	Improved system security (A&AC)	Near-term	Low
Source: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml					
Description: The Organization for the Advancement of Structured Information Standards (OASIS) had promulgated a standard for expressing authorization policies in XML called eXtensivel Access Control Markup Language (XACML). Further work needs to be done in creating standards and best practices for adoption and use of this or similar access control languages.					

#	Research Topic*	Program Areas	Impact (Impact Area)	First Commercial Use Timeframe	Research Risk
7	*Technology to defend against "insider" cyber-attacks*	Awareness and Assessment, Preparation and Prevention, Detection and Reaction	Improved ability to prevent, detect, and mitigate cyberattacks from inside personnel (InfoSec, BusCont, A&AC)	Mid-term	Medium
Source: I3P Banking and Finance Sector Workshop, June 24-25, 2002; DoD Insider Threat Mitigation				Funding Est.: $3-7M	Priority: HIGH
Description: Insider cyber-attacks are both more prevalent and can be more devastating to an organization than externally generated attacks. Research needs to be focused on technology relating to preventing, detecting, and responding to insider attacks. Topics may include "strong universal authentication/identification, effective intrusion detection, tools that allow detection of unrecognized threats (unknown viruses, internal misconduct, patterns of fraud), improvements in software and operating systems (fault tolerance, testing methods to allow earlier detection of vulnerabilities), and improvements in security tools and algorithms to increase detection rates while minimizing false alarms."					

#	Research Topic*	Program Areas	Impact (Impact Area)	First Commercial Use Timeframe	Research Risk
8	*Security procedures to defend against "insider" cyber-attacks*	Awareness and Assessment, Preparation and Prevention, Detection and Reaction	Improved ability to prevent, detect, and mitigate cyber attacks from inside personnel (InfoSec, BusCont, A&AC)	Near-term	Low
Source: I3P Banking and Finance Sector Workshop, June 24-25, 2002; DoD Insider Threat Mitigation				Funding Est.: $1-3M	Priority: HIGH
Description: Insider cyber-attacks are both more prevalent and can be more devastating to an organization than externally generated attacks. Although there are many existing "best practices" for reducing the threat of insider cyber-attacks, research is needed into improved ways of disseminating and implementing these.					

#	Research Topic*	Program Areas	Impact (Impact Area)	First Commercial Use Timeframe	Research Risk
9	*Wireless sensor networks*	Detection and Reaction	Improved security of CIP assets (InfoSec)	Mid-term	Medium
Source: Multiple sources					
Description: Current research on wireless sensor networks has opened new frontiers of environment monitoring and surveillance, e.g. of critical financial and banking center operations. Wireless sensors can control doors, tag computers, operate cameras and other monitoring device to provide security information remotely. Research would focus on applications relevant to the financial and banking sector.					

#	Research Topic*	Program Areas	Impact (Impact Area)	First Commercial Use Timeframe	Research Risk
10	*High reliability biometric identification systems*	Preparation and Prevention	Improved security for the enterprise and computer systems (A&AC)	Mid-term	Medium
Source: Multiple sources				Funding Est.: greater than $7M	Priority: HIGH
Description: Biometric identification systems span a number of technologies. As of yet, none of these systems has achieved the right balance of reliability, security, cost, and ease of use. Continued research is required in all areas to achieve high reliability (both positive and negative) at low cost.					

#	Research Topic*	Program Areas	Impact (Impact Area)	First Commercial Use Timeframe	Research Risk
11	*Gait recognition*	Preparation and Prevention, Detection and Reaction	More reliable detection of potential criminal or terrorist activity (A&AC)	Long-term	Medium
Source: Multiple sources					
Description: Gait or walking patterns are one example of a biometric that shows promise for uniquely detecting individuals. Research into detecting gait patterns related to threat activity will be of use in the financial and banking sector in relation to physical security of critical infrastructure.					

#	Research Topic*	Program Areas	Impact (Impact Area)	First Commercial Use Timeframe	Research Risk
12	*Identifying people in cyberspace*	Preparation and Prevention, Detection and Reaction	Improved trust in cyber-transactions and relationships (A&AC)	Long-term	Medium
Source: I3P Banking and Finance Sector Workshop, June 24-25,2002 (I3P Cyber Security R&D Agenda); NRC Making the Nation Safe					
Description: Just as techniques are needed for uniquely identifying individuals in person, techniques are similarly needed for uniquely identifying individuals in cyberspace if commercial transactions are to proceed smoothly. Research is needed into approaches for identifying individuals across institutions, networks, and geographies, without referring to a central authority. "Trust models" must be defined given the dynamic nature of such relationships. Any such models and approaches have to scale to fit the needs of the national financial and banking sector.					

#	Research Topic*	Program Areas	Impact (Impact Area)	First Commercial Use Timeframe	Research Risk
13	*Asset movement pattern recognition*	Detection and Reaction	Reduce the use of the financial system for terrorist activities (A&AC)	Near-term	Medium
Source: Multiple sources				Funding Est.: $3-7M	Priority: HIGH

Description:
Terrorist organizations require significant financial resources to fund their activities, from recruiting to training to specific acts. Individuals and otherwise legitimate organizations make use of a wide variety of money laundering techniques to provide funding to such organizations.

Research is needed in techniques for detecting suspicious use of the financial system for transferring money or other assets in pursuit of terrorism. Research may include advanced data mining, pattern recognition, and related techniques for detection of money laundering and other money movement activity, including ways to "anonymize" transaction records to ensure appropriate levels of privacy. Pattern recognition techniques currently used in other domains may have applicability.

#	Research Topic*	Program Areas	Impact (Impact Area)	First Commercial Use Timeframe	Research Risk
14	*Quantum encryption*	Preparation and Prevention	Increased data security and privacy (InfoSec)	Mid-term (2-3 years)	Medium
Source: Multiple sources					

Description:
Most new encryption methods discovered in the past decade have based their security on the fact that it would be too costly for current computer technology to be used to crack them. Current computer technology, however, has continued to expand at a rate where more and more secure encryption methods are constantly required.

Research is needed into extremely secure encryption technology not subject to cracking simply by applying more processing power.

#	Research Topic*	Program Areas	Impact (Impact Area)	First Commercial Use Timeframe	Research Risk
15	*Business continuity strategies*	Policy and Strategy, Recovery and Restoration	Improved ability to recover from cyber-attacks (BusCon, BP)	Near-term	Low
Source: Multiple sources				Funding Est.: $1-3M	Priority: HIGH

Description:
The development of business continuity plans is of high importance to organizations in the financial and banking sector. Plans must be developed that allow organizations to implement business continuity strategies in the event of one or multiple simultaneous disasters. However, there are significant questions regarding whether current strategies and plans will achieve this objective.

Research is needed into strategies and plans for recovering from cyber-attacks that are (1) cost-effective, and (2) have a high likelihood that the strategies and plans will be appropriately implemented. Research is needed to develop strategies that will determine the minimal operational requirements of an organization and how these requirements can be achieved after an attack. Issues related to outsourcing of critical services must also be addressed.

#	Research Topic*	Program Areas	Impact (Impact Area)	First Commercial Use Timeframe	Research Risk
16	*Data replication technology*	Preparation and Prevention, Recovery and Restoration	Allows more dispersed backup sites (BusCon)	Near-term	Medium
Source: Multiple sources, Hitachi white paper.				Funding Est.: $3-7M	Priority: HIGH

Description:
Advances in data replication technology are required to provide adequate database synchronization among backup computer sites that may be separated by distances in excess of a hundred miles. Regardless of technology used, the ability to recover and/or reconstruct data after a disaster is paramount in restoring the business operations.

Research is needed that will lead to technology improvements in the areas of data synchronization, data integrity, and data recoverability and reconstruction.

#	Research Topic*	Program Areas	Impact (Impact Area)	First Commercial Use Timeframe	Research Risk
17	*Data replication best practices*	Recovery and Restoration	Provide guidelines to assist organizations in developing their top level disaster recovery requirements	Near-term	Low
Source: Multiple sources				Funding Est.: $1-3M	Priority: HIGH
Description: Selection of recovery time objective (RTO) and recovery point objective (RPO) for critical business processes is complex and greatly affects the cost of disaster recovery solutions. Distance between locations for production and backup operations greatly affects the options available and the cost of disaster recovery operations. Organizations need a framework for making these and other decisions regarding data replication approaches in the context of sound business practices.					

#	Research Topic*	Program Areas	Impact (Impact Area)	First Commercial Use Timeframe	Research Risk
18	*Data decontam-ination approaches*	Recovery and Restoration	Improved data restoration after attack (BusCon)	Mid-term	Medium
Source: NRC Making the Nation Safe					
Description: "Unlike a [database] restore operation used to recreate a clean system after a failure, reconstitution [of data after an attack] requires an additional step: decontamination, which is the process of distinguishing clean system state (unaffected by the intruder) from the portions of infected system state, and eliminating the causes of those differences. Because system users would prefer that as little good data as possible be discarded, this problem is quite difficult. Research is need to create "new decontamination approaches for discarding as little good data as possible, and for removing active and potential infections, on a system that cannot be shut down for decontamination."					

#	Research Topic*	Program Areas	Impact (Impact Area)	First Commercial Use Timeframe	Research Risk
19	*Clearing systems inter-operability*	Preparation and Prevention, Recovery and Restoration	Allows different clearing organizations to provide mutual backup service to their customers (NetProt, BusCont)	Near-term	Low
Source: Interagency Paper on Sounds Business Practices…				Funding Est.: $1-3M	Priority: HIGH
Description: Rather than clearing and settling all financial transactions between two parties, many types of transactions (such as purchase and sale of almost all types of securities, large money transfers, and the like) are cleared through intermediary organizations and systems which serve in the roles of communication networks or clearinghouse or both. In many cases, a financial institution may use only a single clearinghouse for a particular type of transaction, potentially leading to significant system-wide vulnerabilities in the event of a disaster. Example: FedWire and CHIPS both provide clearing services but use different communications formats, protocols, and networks. Some banks have connections to both networks, but often do not have the capability of shifting traffic from one to the other due to the lack of standardization. Research is needed into the definition and cost/benefit of implementing common protocols which would allow clearing system interoperability for various types of financial transactions.					

#	Research Topic*	Program Areas	Impact (Impact Area)	First Commercial Use Timeframe	Research Risk
20	*Common XML frameworks financial transactions*	Preparation and Prevention	Increased ability to have alternative systems for backup (BusCont); increased ability to analyze financial transactions for patterns (InfoSec)	Near-term	Low
Source: http://lighthouse-partners.com/xml/					
Description: To facilitate using different organizations for trading, clearing, and settlement, common XML frameworks need to be developed and agreed upon across the industry. For example, although FIX is an accepted standard for securities trading, different organizations have implemented different aspects of the protocol. FIX-XML (FIXML) frameworks are being added to the standard to facilitate the standard adoption Additional frameworks need to be developed for additional types of transactions and procedures need to be developed for encouraging adoption.					

#	Research Topic*	Program Areas	Impact (Impact Area)	First Commercial Use Timeframe	Research Risk
21	*Best practices repository*	Preparation and Prevention	Information sharing (BP)	Near-term	Low
Source: Multiple sources				Funding Est.: less than $1M	Priority: HIGH
Description: Create a best practices and standards repository available for members of the financial and banking sector via the web. Industry, enterprise, system and process practices and standards should be sought out, summarized, categorized, indexed, and made available to the community. Example: DOJ standards registry (http://it.ojp.gov/jsr/public/index.jsp)					

#	Research Topic*	Program Areas	Impact (Impact Area)	First Commercial Use Timeframe	Research Risk
22	*Patch clearinghouse*	Preparation and Prevention	Information sharing (BP)	Near-term	Low
Source: National Strategy AR 2-7; NRC Making the Nation Safe				Funding Est.: $1-3M	Priority: HIGH
Description: Financial organizations use software from many different vendors. Vendors typically provide annual releases of this software to organizations that are on paid maintenance plans, but also develop multiple interim "patches" that are only distributed to organizations that specifically inquire. Often these patches have to do with correcting security flaws. Creating a "patch clearinghouse" available to all organizations in the sector will help ensure that important software updates become known to the community on a timely basis. Establishment of uniform rating system for severity of problems or importance of patch will help organizations set priorities for implementing patches. A contributory database listing effective patch sets across multiple software systems will assist all participants in deciding which patches to use. An independent patch testing agency will help establish the trustworthiness of patches in different operational environments.					

#	Research Topic*	Program Areas	Impact (Impact Area)	First Commercial Use Timeframe	Research Risk
23	*Life-cycle costing*	Risk Management	Improve the ability of organizations to implement cost-effective CIP solutions (BP)	Near-term	Low
Source: EC Comprehensive Roadmap: Analysis and Assessment for CIP; Giga Information Report				Funding Est.: less than $1M	Priority: HIGH
Description: One of the key issues in the adoption of improved CIP technology is the ability of organizations to fully understand the costs and benefits. Research is needed on life-cycle costs of CIP technologies and the creation of cost-benefit models that can be used in organizational decision making.					

#	Research Topic*	Program Areas	Impact (Impact Area)	First Commercial Use Timeframe	Research Risk
24	*Creating public policy to promote improved critical infrastructure protection*	Policy and Strategy	Reduce the gap between "state of the art" and "state of the practice" in employing best practices (BP)	Near-term	Medium
Source: NRC Making the Nation Safer				Funding Est.: less than $1M	Priority: HIGH
Description: Market forces have not yet provided sufficient incentive for banks and financial organizations to uniformly adopt the best technologies and practices available for critical infrastructure protection, including security and business continuity. This means that there is a range of implementation with some organizations significantly below the state-of-the-art. Improving the overall resiliency of the finance and banking sector requires the development of public policies that encourage implementation of such best practices and technologies to the goal of significantly improved critical infrastructure protection.					

#	Research Topic*	Program Areas	Impact (Impact Area)	First Commercial Use Timeframe	Research Risk
25	*Standards for end-to-end testing of industry backup systems*	Preparation and Prevention; Recovery and Restoration	Ensure efficacy of industry-wide backup systems (BusCont)	Near-term	Low
Source: Multiple sources				Funding Est.: less than $1M	Priority: HIGH
Description: The ability of key components of the finance and banking sector to continue to function in the face of a major disaster will be largely dependent on how well the various back-up systems are able to communicate with one another. This takes in more than just the ability to establish and maintain communication; it also includes the capability to conduct transactions at a volume and level of accuracy sufficient to maintain confidence in the system.					

#	Research Topic*	Program Areas	Impact (Impact Area)	First Commercial Use Timeframe	Research Risk
26	*Implications of industry outsourcing*	Policy and Strategy; Risk Management	Better understanding of outsourcing effects (3rd Party, BusCont, BP)	Near-term	Low
Source: Multiple sources				Funding Est.: Less than $1M	Priority: High
Description: There is an expanding trend in the industry to outsource various functions, particularly those related to networks and information systems. The implications of this trend for cyber-security, business continuity, and overall risk management have yet to be investigated.					

#	Research Topic*	Program Areas	Impact (Impact Area)	First Commercial Use Timeframe	Research Risk
27	*Tracking physical diversity of telecommuni-cations circuits*	Preparation and Prevention; Detection and Discovery; Recovery and Restoration	Improved resiliency of financial services telecommunications	Near-term	Low
Source: Federal Reserve Board, National Telecommunications System				Funding Est.:	Priority:

Description:
In order to have an effective continuity of operations plan, many financial institutions have sought to obtain true physical diversity in critical and back-up telecom services as a way of ensuring rapid recovery from service disruptions. These circuits often qualify for and are registered under the National Communications System's (NCS) Telecommunications Service Priority (TSP) program for restoration and emergency provisioning. "Physical diversity" requires that the two circuits are sufficiently far apart at all points such that an incident that disrupts one circuit is unlikely to affect the other (e.g. not in the same conduit, along either side of the same railroad track or bridge, located in same telecom hotel). The events of Sept 11th brought to light the fact that diversity frequently is not maintained during routine telecom business processes (e.g., grooming, technology upgrades & other engineering changes) because many service providers have not developed protocols for tracking and maintaining circuit diversity. In addition, it is even more difficult to assure diversity of critical circuit pairs when different telecom providers are supplying circuits.

TSP circuit registration provides a basis for tracking circuits that are critical to the National Security and Emergency Preparedness (NS/EP) of the United States. It may be possible to use the TSP program for tracking NS/EP circuits as a basis for also tracking pairs of critical circuits through an expansion of the information maintained on circuit registration records.

Research is needed on ways to track diversity of NS/EP circuit pairs and protocols for maintaining diversity across telecom providers. Research should consider the need for an automated data base that identifies paired circuit information; establishing uniform procedures for preserving diversity; and use of real-time data update procedures (e.g., use of hand-held data collection devices) to assure that normal grooming and other types of engineering processes do not erode physical diversity. This analysis could recommend several major improvements to the TSP program – or development of a multi-provider circuit diversity tracking program that includes standardized protocols for marking and maintaining pairs of diverse circuits.

Explanation of Column Headings:

#	*Research Topic*	*Program Areas*	*Impact (Impact Area)*	*First Commercial Use Timeframe*	*Research Risk*
28	*Wide-spread identity theft*	Preparation and Prevention; Detection and Discovery; Recovery and Restoration	Information security and privacy (InfoSec)	Mid-term	Medium
Source: Multiple sources				Funding Est.: $1-3M	Priority: High

Description:
Identity theft is a form of attack that has been primarily used for fraudulent gain and is not yet commonly recognized as an infrastructure attack. As identity theft becomes more widespread and flagrant, however, it may become a basis for broader and more far reaching interruption to the finance and banking sector. Further, new initiatives such as centralized identity databases with biometric information may increase the severity of such attacks.

Research is required into prevention, detection, impact, and response to wide-spread identify theft attacks.

Research Topic	Brief title for research project
Program Areas	R&D activities can focus on one or more aspects of the CIP life-cycle, from policy and strategy to recovery and restoration of business activities.
Impact (Impact Area)	Expected impact in improving resiliency of the finance and banking sector (business practice or technology characteristic impacted)
Timeframe	Expected time frame both of research project and of development into products or services in use in industry.
Research Risk	Indication of whether this is “developmental” research, with results that are highly likely (low risk), “initial” research, with results that are very uncertain (high risk), or somewhere in between.
Source	Data or interview sources
Priority	Importance within the Treasury CIP-CP R&D program.
Funding Est.	Rough order of magnitude to initiate a research program designed to show practical results. Total funding to be determined during early project stages.
Description	Short description or examples of expected research projects.

Source material:

National Strategy:

1. "The National Strategy to Secure Cyberspace," The White House, February 2003. [http://www.dhs.gov/interweb/assetlibrary/National_Cyberspace_Strategy.pdf]
2. "Banking and Finance Sector, The National Strategy for Critical Infrastructure Assurance," May 13, 2002. [https://www.pcis.org/getDocument.cfm?urlLibraryDocID=39]
3. "Banking and Finance Sector, Compendium of Supporting Documents to The National Strategy for Critical Infrastructure Assurance," May 13, 2002. [http://www.pcis.org/getDocument.cfm?urlLibraryDocID=38]
4. "Comments on Draft National Strategy to Secure Cyberspace," BITS (Financial Services Roundtable), December 20, 2002.
5. "Report on the Federal Agenda in Critical Infrastructure Protection Research and Development: Research Vision, Objectives, and Programs," Critical Infrastructure Protection R&D Interagency Working Group, January 2001
6. "The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets," The White House, February 2003. [http://www.dhs.gov/interweb/assetlibrary/Physical_Strategy.pdf].

Interagency White Paper:

7. "Comments on Draft Interagency White Paper on Sounds Practices to Strengthen the Resilience of the U.S. Financial System," BITS October 21, 2002.
8. "Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System," from the Board of Governors of the Federal Reserve System, Comptroller of the Currency, and the Securities and Exchange Commission (Release 34-47638). [http://www.federalreserve.gov/boarddocs/press/bcreg/2003/20030408/attachment.pdf]

Federal Financial Institution Examination Council:

9. "FFIEC Information Technology Examination Handbook." [http://www.ffiec.gov/ffiecinfobase/index.html]

Institute for Information Infrastructure Protection (I3P):

10. "Cyber Security Research and Development Agenda," Institute for Information Infrastructure Protection (I3P), January 2003. [http://www.thei3p.org/documents/2003_Cyber_Security_RD_Agenda.pdf]
11. "Comments on the draft I3P's 2003 Cyber Security Research and Development Agenda," BITS (Financial Services Roundtable), December 6, 2002.
12. "National Information Infrastructure Protection Research and Development Agenda Initiative Report: Information Infrastructure Protection: Survey of Research and Development,"I3P, September 9, 2002.
13. "National Information Infrastructure Protection Research and Development Agenda Initiative Report: Information Infrastructure Protection: Survey of Related Roadmaps and R&D Agendas," I3P, September 9, 2002.
14. Report of the I3P Banking and Finance Sector Workshop, June 24-25,2002, Rand Corporation

Other R&D Agendas:

15. "Preliminary R&D Roadmap for Protecting and Assuring Critical National Infrastructures," Transition Office of the President's Commission on Critical Infrastructure Protection and the Critical Infrastructure Assurance Office, July, 1998. [http://www.ciao.gov/resource/roadmap-main.pdf]
16. "National Scale INFOSEC Research Hard Problems List," The INFOSEC Research Council, November 2001. [http://www.infosec-research.org/docs_public/IRC-HPL-as-released-990921.doc]
17. "Critical Infrastructure Protection: Significant Challenges in Developing National Capabilities," General Accounting Office Report GAO-01-323 to the Subcommittee on Technology, Terrorism, and Government Information, Committee on the Judiciary, U.S. Senate, April 2001.
18. "Information Technology," Chapter 5 in *Making the Nation Safer: The Role of Science and Technology in Countering Terrorism* Report of the National Research Council, National Academy of Sciences. [http://www.nap.edu/books/0309084814/html/]

GAO Reports:

19. "Critical Infrastructure Protection: Efforts of the Financial Services Sector to Address Cyber Threats," General Accounting Office Report GAO-03-173 to the Subcommittee on Domestic Monetary Policy, Technology, and Economic Growth, Committee on Financial Services, House of Representatives, January 2003.
20. "Critical Infrastructure Protection: Significant Challenges Need to Be Addressed," General Accounting Office Report GAO-02-961T to the Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations, Committee on Government Reform, House of Representatives, July 2002.
21. "Information Security: Effective Patch Management is Critical to Mitigating Software Vulnerabilities," General Accounting Office Report GAO-03-1138T to the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, Committee on Government Reform, House of Representatives, September 2003. [http://www.gao.gov/new.items/d031138t.pdf]

National Institute of Standards and Technology:

22. "Risk Management Guide for Information Technology Systems," Recommendations of the National Institute of Standards and Technology, Publication 800-30, October, 2001. [http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf]
23. "General Accepted Principles and Practices for Securing Information Technology Systems," Recommendations of the National Institute of Standards and Technology, Publication 800-14, September, 1996. [http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf]

European Community:

24. "R&D Strategy Roadmap: Background Paper," Dependability Development Support Initiative (DDSI), European Community Information Security Technology Programme, August 2002.

25. "Toward a dependable Information Infrastructure for the EU," Andrea Servida, European Commission,
26. "A Dependability Roadmap for the Information Society in Europe," Accompanying Measure System Dependability Project, Information Societies Technology Programme, European Commission, Draft 3, March 31, 2003.
27. "Comprehensive Roadmap: Analysis and Assessment for Critical Infrastructure Protection (ACIP)," Information Society Technology Programme, European Commission, May, 2003. [http://www.iabg.de/acip/doc/wp6/_vti_cnf/D64_roadmap.pdf] "DoD Insider Threat Mitigation, Final Report," DoD Insider Threat Integrated Process Team, April 24, 2000.

Specific topics:

28. "Financial Services Sector Coordination: A Public/Private Partnership," presentation by Rhonda MacLean to the Business Continuity Planning Conference, Securities Industry Association, October 30, 2002.
29. "Providing a Security Framework for Critical Infrastructure Sectors and Enterprise Organizations," Presentation of American Security Consortium, 2003.
30. "Cybershield," Presentation by SRI International, 2003.
31. "Core Security: Preventing Attacks on Hosts and Data," White Paper, Vormetric Corporation, 2003.
32. "National Biometric Security Project," presentation by John Seidlarz to the 18th National Defense Industrial Association Security Division Symposium, June 27, 2002. [http://www.dtic.mil/ndia/2002security/siedlarz.pdf]
33. "Risk Management Principles for Electronic Banking," Basel Committee on Banking Supervision, May, 2001. [http://www.bis.org/publ/bcbs82.pdf]
34. "BITS Framework: Managing Technology Risk for Information Technology Service Provider Relationships," BITS (Financial Services Roundtable), October, 2001. [http://www.bitsinfo.org/FrameworkVer32.doc]
35. "Emerging Standards: Easing the Complexity of Managing Storage," Storage Networking Industry Association, 2003.
36. "Getting the message," IEEE Spectrum, April 2003.
37. "Disaster Recovery Issues and Solutions," Hitachi Data Systems, March, 2002.
38. "The IT Security Market Is Not What IT Used To Be," Steve Hunt, Giga Information Group, Inc. 2003. [http://www.csoonline.com/analyst/report1323.html]
39. "Securing Storage Networks," @stake Research Report, April, 2003. [http://www.atstake.com/research/reports/acrobat/atstake_storage_networks.pdf]
40. "Business Continuity Planning: A 2002 Roundup," Securities Industry Association Research Report, Vol. III, No. 11, December 27, 2002. [http://www.sia.com/research/pdf/RsrchRprtVol3-11.pdf]
41. "Evaluating Intrusion Detection Systems," Symantec. June 17, 2003. [http://enterprisesecurity.symantec.com/article.cfm?articleid=2284&EID=414]
42. "Newsblaster Project," Columbia University [http://www1.cs.columbia.edu/nlp/newsblaster/faq.html]