The Homeland Security Front

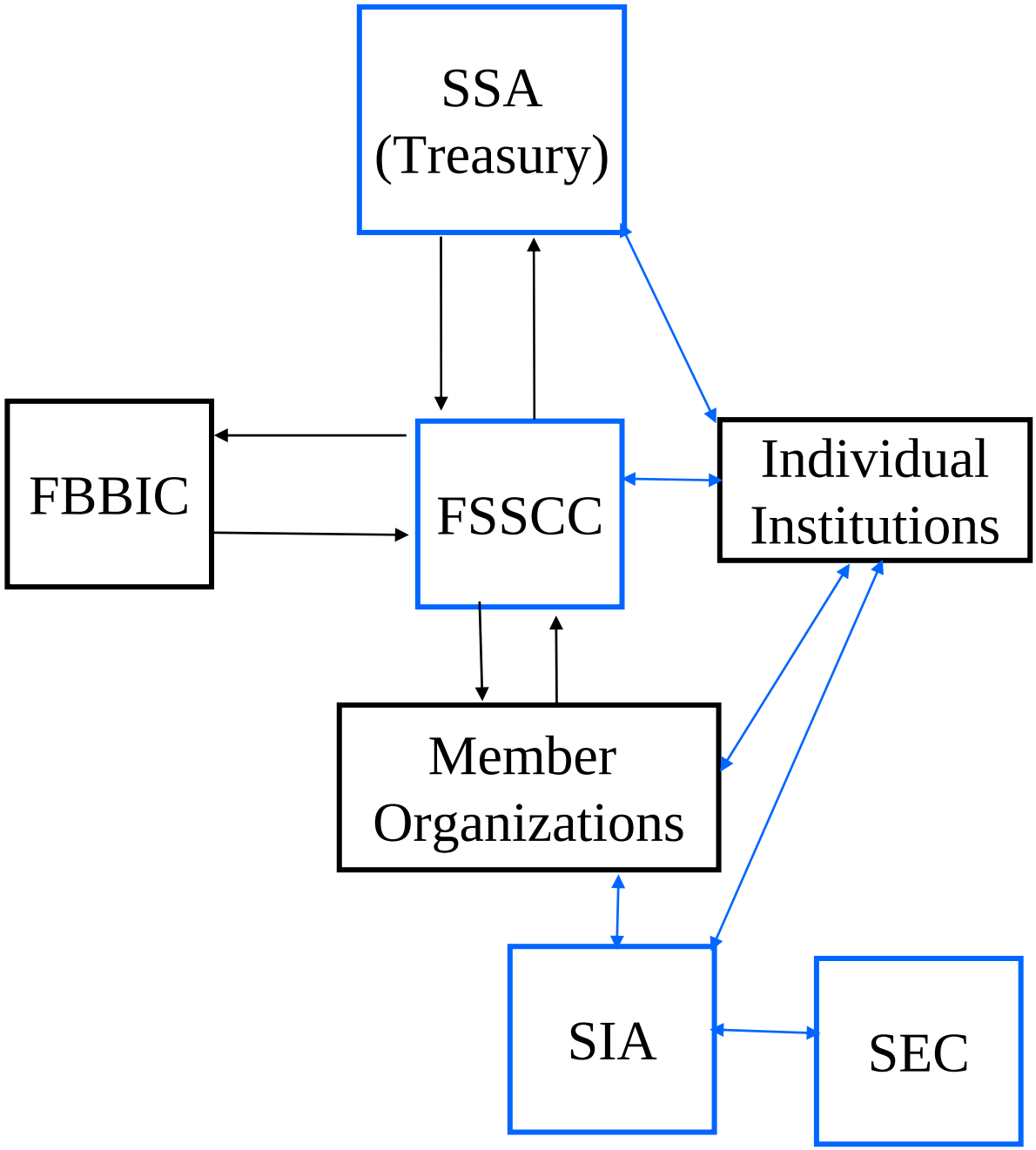
SIA Internal Audit Division
Annual Conference
October 16, 2006

Jennifer Bayuk
Chief Information Security Officer, Bear Stearns
Chair, SIA Information Security Sub-Committee
Chair, Financial Services Sector Coordinating Council
R&D Committee

Glossary

CI/KR:	Critical Infrastructure, Key Resources
CIP:	Critical Infrastructure Protection
DHS:	Department of Homeland Security
FIBBC:	Financial and Banking Information Infrastructure Committee
FSSCC:	Financial Services Sector Coordinating Council
HLS:	Homeland Security
NIPP:	National Infrastructure Protection Plan
SSA:	Sector Specific Agency

Securities Industry Players



Note that the financial industry is dominated by banking interests, so pure Securities Industry players have a narrower field of focus than the entire DHS-FI establishment.

FBBIC

BEAR STEARNS

Mission:

- The President's Critical Infrastructure Protection Board recommended the following mission statement for the FBIIC: "Working with appropriate members of financial institution regulatory agencies, coordinate efforts to improve the reliability and security of financial information infrastructure."

Strategy:

- 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.

Members:

- Commodity Futures Trading Commission
- Conference of State Bank Supervisors
- Department of the Treasury
- Farm Credit Administration
- Federal Deposit Insurance Corporation
- Federal Housing Finance Board
- Federal Reserve Bank of New York
- Federal Reserve Board
- National Association of Insurance Commissioners
- National Association of State Credit Union Supervisors
- National Credit Union Administration
- North American Securities Administrators Association
- Office of the Comptroller of the Currency
- Office of Federal Housing Enterprise Oversight
- Office of Thrift Supervision
- Securities and Exchange Commission
- Securities Investor Protection Corporation

FSSCC

BEAR STEARNS

Mission:

- To foster and facilitate the coordination of financial services sector-wide voluntary activities and initiatives designed to improve Critical Infrastructure Protection and Homeland Security.

Strategy:

- Provide broad industry representation for CIP/HLS and related matters for the financial services sector and for voluntary sector-wide partnership efforts.
- Foster and promote coordination and cooperation among participating sector constituencies on CIP/HLS related activities and initiatives.
- Identify voluntary efforts where improvements in coordination can foster sector preparedness for CIP/HLS.
- Establish and promote broad sector activities and initiatives that improve CIP/HLS.
- Identify barriers to and recommend initiatives to improve sector-wide voluntary CIP/HLS information and knowledge sharing and the timely dissemination processes for critical information sharing among all sector constituencies.
- Improve sector awareness of CIP/HLS issues, available information, sector activities/initiatives and opportunities for improved coordination.

Members:

America's Community Bankers
American Bankers Association
American Council of Life Insurers
American Insurance Association
American Society for Industrial Security (ASIS) International
BAI
BITS/The Financial Services Roundtable
ChicagoFIRST, LLC
Chicago Mercantile Exchange
CLS Group
Consumer Bankers Association
Credit Union National Association
The Depository Trust & Clearing Corporation (DTCC)
Fannie Mae
Financial Information Forum
Financial Services technology Forum
Fin Svcs Info Sharing & Anal Center (FS/ISAC)
Futures Industry Association
Independent Community Bankers of America
Investment Company Institute
Managed Funds Association
The NASDAQ Stock Market, Inc.
National Association of Federal Credit Unions
National Association of Securities Dealers (NASD)
NACHA — The Electronic Payments Association
New York Board of Trade (NYBOT)
The Clearing House
Securities Industry Association (SIA)
Securities Industry Automation Corporation (SIAC)
The Bond Market Association
The Options Clearing Corporation
VISA USA Inc

Financial Infrastructure Protection Roles and Responsibilities

BEAR STEARNS

- Department of Homeland Security: Manage the Nation's overall CI/KR protection framework and oversee NIPP development and implementation.
- Treasury, the Sector-Specific Agency: Implement the NIPP framework and guidance as tailored to the specific characteristics and risk landscapes of the Financial Services Industry.
- Other Federal Departments, Agencies, and Offices: Implement specific CI/KR protection roles designated in HSPD-7 or other relevant statutes, executive orders, and policy directives.
- State, Local, and Tribal Governments: Develop and implement a CI/KR protection program as a component of their overarching homeland security programs.
- Regional Partners: Use partnerships that cross jurisdictional and sector boundaries to address CI/KR protection within a defined geographical area.
- Boards, Commissions, Authorities, Councils, and Other Entities, e.g. SIA: Perform regulatory, advisory, policy, or business oversight functions related to various aspects of CI/KR operations and protection within and across sectors and jurisdictions.
- Private Sector Owners and Operators of Banks, Exchanges, Clearing Houses, etc: Undertake CI/KR protection, restoration, coordination, and cooperation activities, and provide advice, recommendations, and subject matter expertise to the Federal Government;
- Homeland Security Advisory Councils: Provide advice, recommendations, and expertise to the government regarding protection policy and activities.
- Academia and Research Centers: Provide CI/KR protection subject matter expertise, independent analysis, research and development (R&D), and educational programs.

NIPP Roadmap

BEAR STEARNS

Notes: X = Primary responsibility O = Support responsibility (may be required to qualify for grants)
+ = Milestone indicator NLT = Not later than

Chapter	Implementation Actions	Milestone				Security Partner					
		NLT 90 Days After NIPP Approval	NLT 180 Days	NLT 365 Days	Specific Date	DHS	Sector-Specific Agency	Other Federal Agency	State or Territory	Local and Tribal	Private Sector
2	**AUTHORITIES, ROLES, AND RESPONSIBILITIES**										
	Review NIPP and establish processes needed to support NIPP implementation.	+				X	X	X	X	X	X
	Incorporate NIPP into strategies for cooperation with foreign countries and international/multinational organizations.		+			X	X	X	O	O	O
3	**THE PROTECTION PROGRAM STRATEGY: MANAGING RISK**										
	Develop sector-specific CI/KR inventory guidance.		+			X	X	O	O	O	O
	Review existing risk assessment methodologies to determine compatibility with the NIPP baseline criteria.		+			X	X	X	X	X	X
	Establish timeline for: (1) the development of sector-specific risk methodologies, and (2) for conducting consequence-based top-screening for all CI/KR sectors.		+			X	X	O	O	O	O
	Conduct and validate consequence assessments of priority CI/KR as identified by the top-screening process.			+		X	X	X	X	X	X
	Conduct or facilitate vulnerability assessments in priority CI/KR sectors and identify cross-sector vulnerabilities.			+		X	X	X	X	X	X
	Develop sector-specific CI/KR threat assessments needed to support comprehensive risk assessments.	+				X	O	O	O	O	O
	Provide guidance on metrics for annual reporting and national-level, cross-sector comparative analysis.	+				X	O	O	O	O	O
4	**ORGANIZING AND PARTNERING FOR CI/KR PROTECTION**										
	Establish all SCCs, GCCs, and SLTGCC in accordance with the NIPP partnership model.	+				X	X	O	O	O	O
	Complete rollout of HSIN-CS COI; implement policies for vetting and disseminating information to security partners.			+		X	X	O	O	O	O
	Identify sector-level information-sharing mechanisms and ensure that information protection practices comply with appropriate guidance for protection of classified or sensitive information. Publish PCII final rule.	+				X	X	O	O	O	O
	Develop Annual CI/KR Protection Information Requirements Report.		+			X	O	O	O	O	O
	Work with the Department of State to review the charter and coordinating mechanisms for the interagency working group that coordinates U.S. international CI/KR protection outreach and update as needed to align with the NIPP.	+				X	X	X	O	O	O

NIPP Plan Continued

BEAR STEARNS

Chapter	Implementation Actions	Milestone				Security Partner					
		NLT 90 Days After NIPP Approval	NLT 180 Days	NLT 365 Days	Specific Date	DHS	Sector-Specific Agency	Other Federal Agency	State or Territory	Local and Tribal	Private Sector
5	**INTEGRATING CI/KR PROTECTION AS PART OF THE HOMELAND SECURITY MISSION**										
	Coordinate SSP development in collaboration with security partners and submit to DHS with appropriate documentation of concurrence.		+			o	x	o	o	o	o
	Review and revise CI/KR-related plans as needed to reinforce linkage between NIPP steady-state CI/KR protection and NRP incident management requirements.		+			x	x	x	x	x	x
	Review current CI/KR protection measures to ensure alignment with HSAS threat conditions and specific threat vectors/scenarios.		+			x	x	x	x	x	x
6	**ENSURING AN EFFECTIVE, EFFICIENT PROGRAM OVER THE LONG TERM**										
	Develop and implement a comprehensive national CI/KR protection awareness program.		+			x	x	o	o	o	o
	Review and, as appropriate, revise training programs to ensure consistency with NIPP requirements.		+			x	x	x	x	x	x
	Provide initial NIPP training to security partners.	+				x	x	o	o	o	o
	Ensure that national exercises include CI/KR protection and interaction between the NIPP and the NRP.	+				x	x	o	o	o	o
	Communicate requirements for CI/KR-related R&D to DHS for use in the national R&D planning effort.				July 1 (Annually)	o	x	x	o	o	o
	Identify all databases, data services and sources, and modeling capabilities with CI/KR application.		+			x	x	x	x	x	x
	Conduct first annual review of the NIPP and SSPs.			+		x	x	x	x	x	x
7	**PROVIDING RESOURCES FOR THE CI/KR PROTECTION PROGRAM**										
	Submit Sector CI/KR Protection Annual Report to DHS				July 1 (Annually)	o	x	o	o	o	o
	Submit National CI/KR Protection Annual Report to the Executive Office of the President.				Sep 1 (Annually)	x	o	o	o	o	o
	Review homeland security grant guidance to ensure that requirements are consistent with the NIPP.	+				x	o	o	o	o	o
	Advise State, local, and tribal governments of SSA grant programs and/or other sources that can support the NIPP.		+			x	x	o	o	o	o
	Apply for homeland security grants to address CI/KR protection efforts per DHS/G&T guidance.				*	o	o	o	x	x	o

NIPP R&D Focus

BEAR STEARNS

Cross-reference to Financial Services R&D Focus:

	NIPP CI/KR Protection R&D Themes									Other R&D Support for CI/KR				Items not in NIPP R&D Focus			
FSSCC Research Agenda	A Detection & Sensor systems	B Protection & Prevention Systems	C Entry & Access Portals	D Insider Threat Detection	E Analysis & Decision Support Systems	F Response, Recovery, & Reconstitution Tools	G Emerging Threats & Vulnerability Analysis Aids	H Advanced Infrastructure Architectures	I Human & Social Issues	J Ensure compatibility of cyber systems with inter-operability standards	K Explore methods to authenticate and verify personal identity	L Coordinate dev of CI/KR protection consensus standards	M Improve technical surveillance, monitoring and detection capabilities	N Information Hiding	O Devaluation and Avoidance	P Business Process Simulation	Q Economics of InfoSec
1. Secure Financial Transaction Protocol (SFTP)		B						H		J	K	L		N			Q
2. Resilient Financial Transaction System (RFTS)	A	B	C			F		H	I			L					
3. Enrollment and Identity Credential Management		B						H	I		K						
4. Suggested Practices and Standards	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
5. Understanding and Avoiding the Insider Threat	A	B		D			G		I				M				
6. Financial Information Tracing and Policy Enforcement		B			E		G	H	I		K		M			P	Q
7. Testing		B					G	H				L					
8. Standards for measuring ROI of CIP and Security Technology					E		G		I								

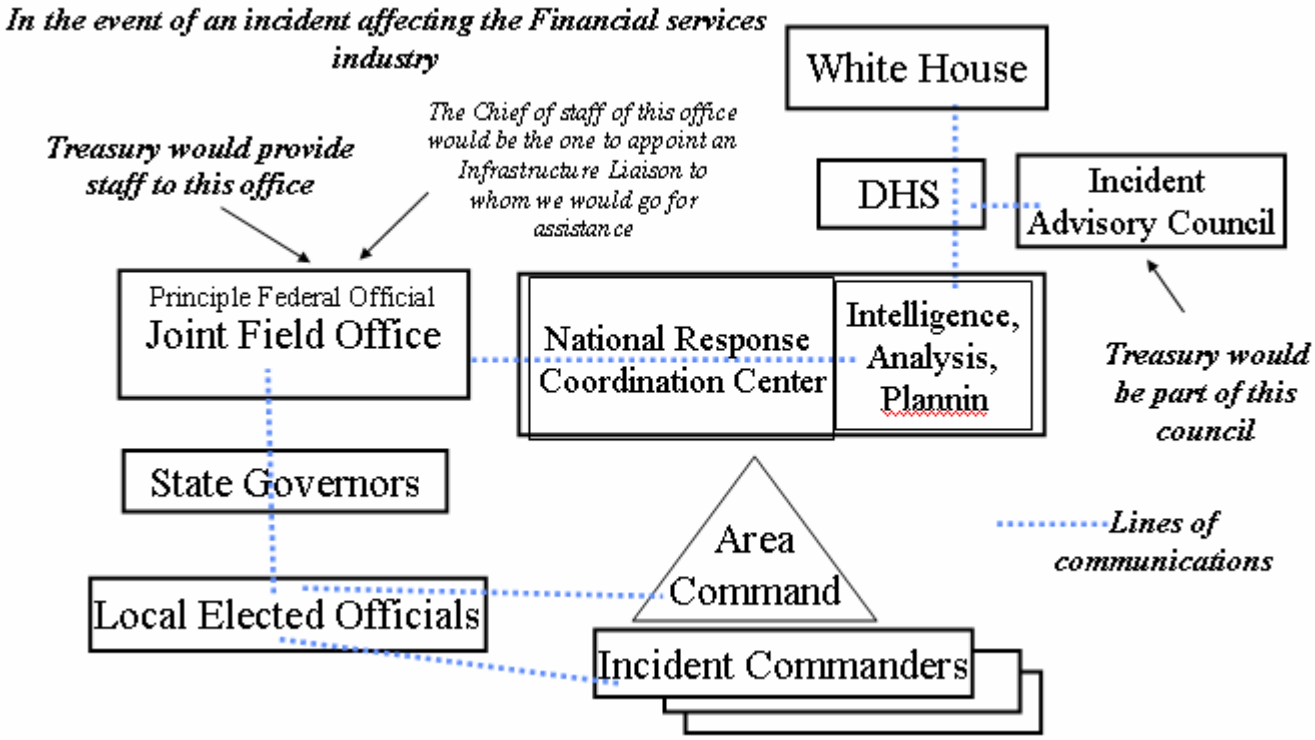
The objective of this mapping is to demonstrate how much the FSSCC R&D Agenda has in common with the NIPP R&D plans and programs, as well as to demonstrate in which aspects they differ. Because this paper combines the opinions of subject-matter experts in homeland security and financial services, the resulting recommendations will meet the needs of both constituencies. It is intended that DHS should use this information tweak its projects to directly address the CI/KR research needs of the Financial Services Industry. This way, the future direction and scope of the NIPP research program will more closely align with the proposed FSSCC R&D Agenda. For example, in the next version of the NIPP, DHS may add new R&D areas of focus that are in the FSSCC document but are not in the current NIPP.

Sector-specific NIPP Plan

BEAR STEARNS

- Treasury has solicited all FSSCC Member organizations to provide input.
- Plan will be drafted by Treasury and circulated back to FSSCC and FBBIC for comment.
- Final draft expected in the November timeframe.
- SIA Contribution:
  - FSSCC Membership
  - FSSCC R&D Committee Membership
  - FS/ISAC Membership
- Any questions about how to deal with Homeland Security activities in the interim may be put to Treasury via the SIA Membership of the FSSCC.

Current Crisis Communication Plan



Securities Industry Communications Mechanism

Current:

- SIA BCP, generally accepted by DOT as model on which to build any future activity

Future:

- As per presidential directive, should evolve to be the FS/ISAC, which will somehow have to be coordinated with SIA BCP

Current Securities Industry Homeland Security Visitors

BEAR STEARNS

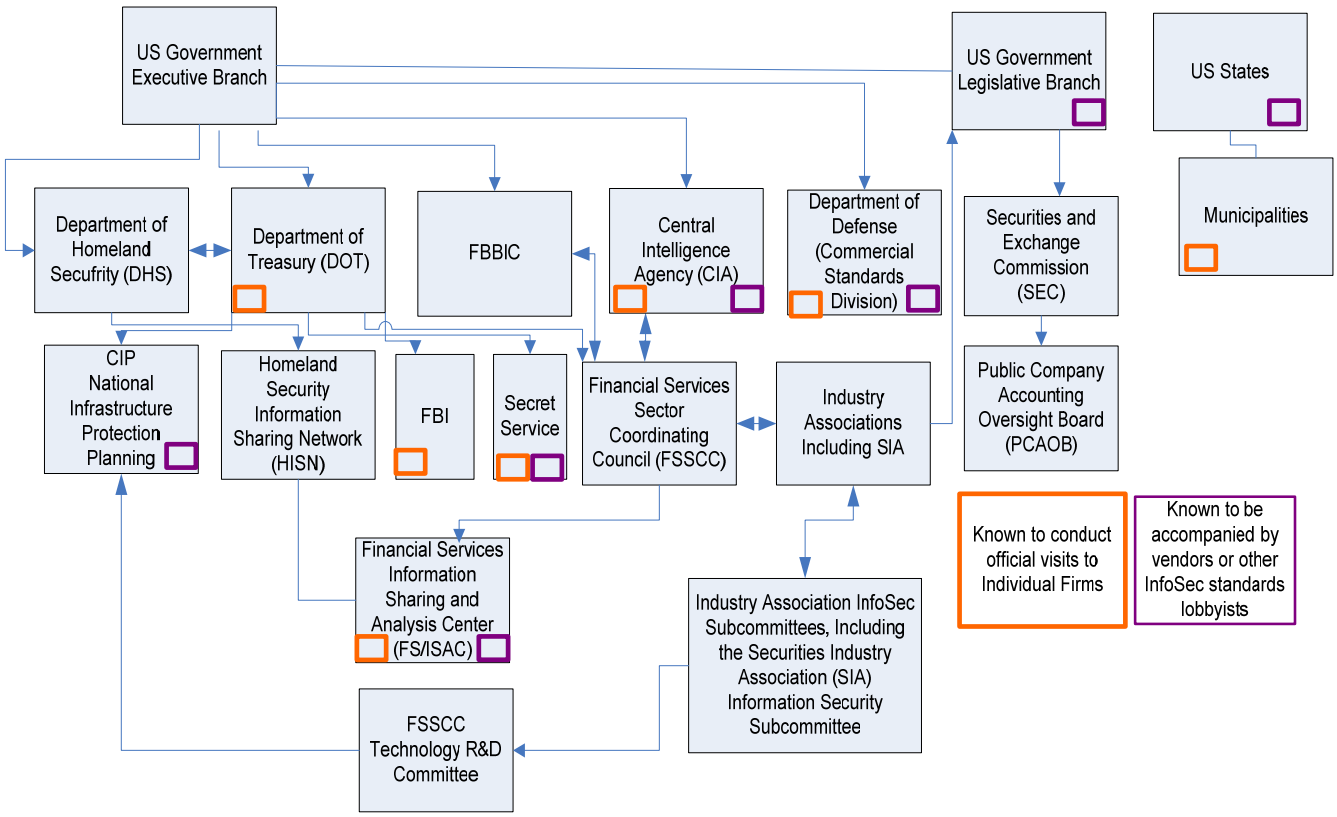
Part of NIPP:

- Local Law Enforcement (to discuss incident response procedures).
- DHS (via DOT and FSSCC to discuss communication, protection and response activities).
- Secret Service (to discuss threats and appropriate response).

Not part of NIPP:

- CIA (To discuss simulation test results).
- DOD (To discuss technology standards for commercial products).
- DHS (via vendors, to discuss application of technology).
- FBI (except in the case of crime investigation).

The Homeland Security Front



Conclusion:

It has been difficult to tell the difference between government visitors and the special interests that would like to set requirements for the Financial Industry.

Close scrutiny of Treasury's SSA NIPP will be required to keep InfoSec security programs focused on actual regulatory compliance.

Discussion