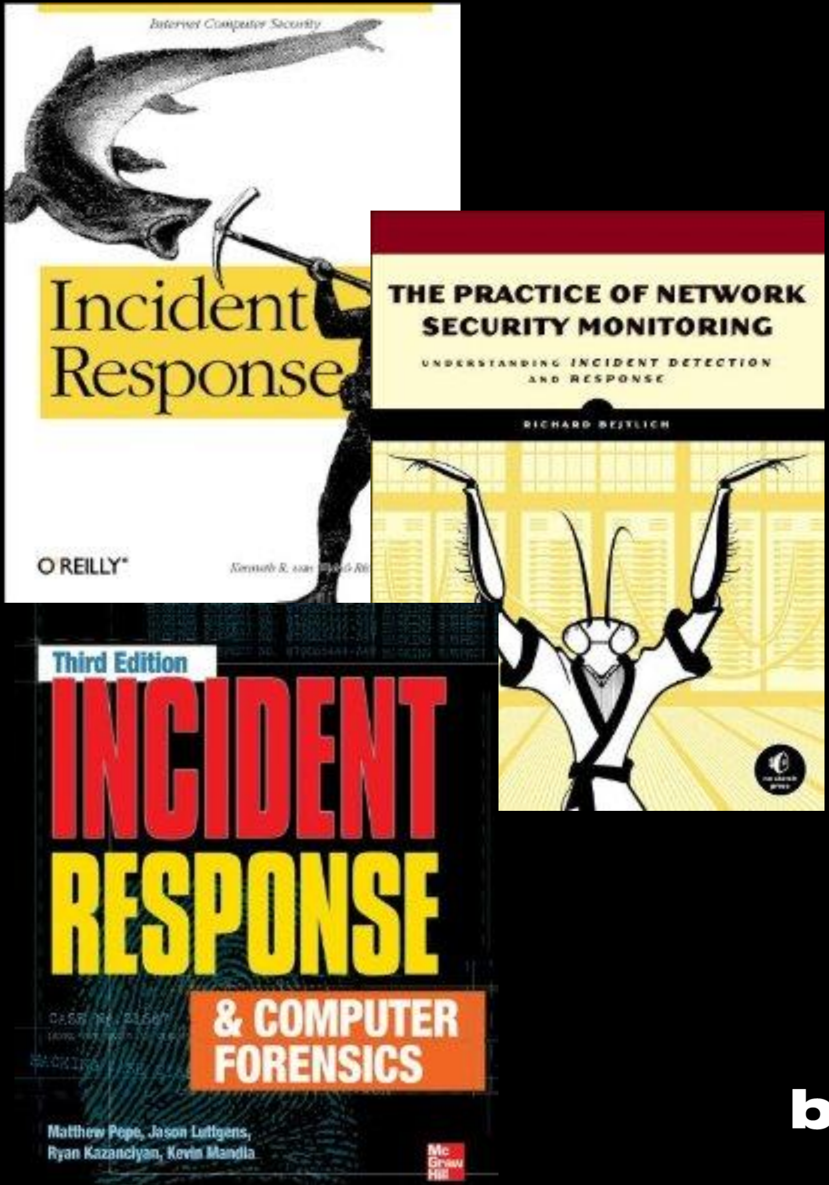
Above My Pay Grade:

Incident Response at the National Level

Jason Healey

Atlantic Council

Traditional Incident Response


Internet Computer Security
Incident Response
O'REILLY
THE PRACTICE OF NETWORK SECURITY MONITORING
UNDERSTANDING INCIDENT DETECTION AND RESPONSE
RICHARD BEJTLICH
Third Edition
INCIDENT RESPONSE
& COMPUTER FORENSICS
Matthew Pepe, Jason Luttgens, Ryan Kazanciyan, Kevin Mandia
Mc Graw Hill

Copyright 2013 tagxedo.com

But at the national level, incident response is a different game

Implications for

- Misunderstandings between geeks and wonks
- Attribution
- Decision making
- Large-scale response (or miscalculations about response)

EXAMPLE:

LARGE SCALE ATTACK ON FINANCE

Large-scale Attack on Finance Sector

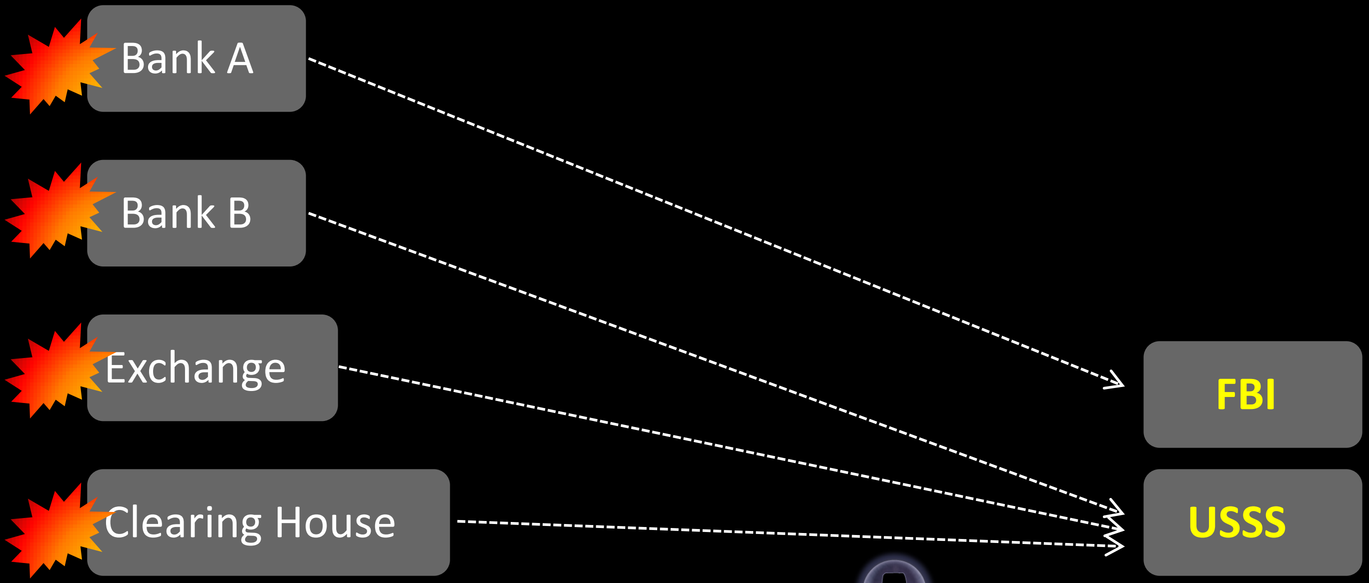
Who Is Their First External Call To?

- Bank A
- Bank B
- Exchange
- Clearing House

First: Call a Law Firm!

Then Mandiant or CrowdStrike!

After That: Tell the Cops…



Bank A

Bank B

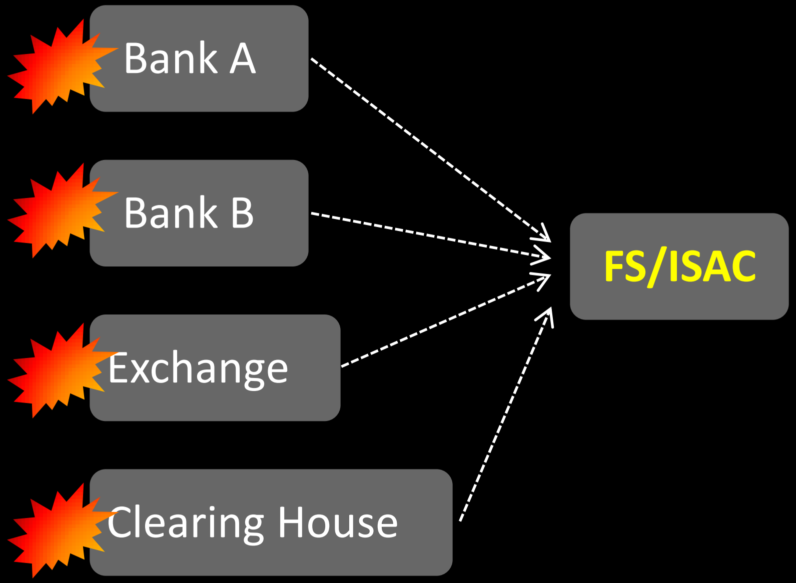
Exchange

Clearing House

FBI

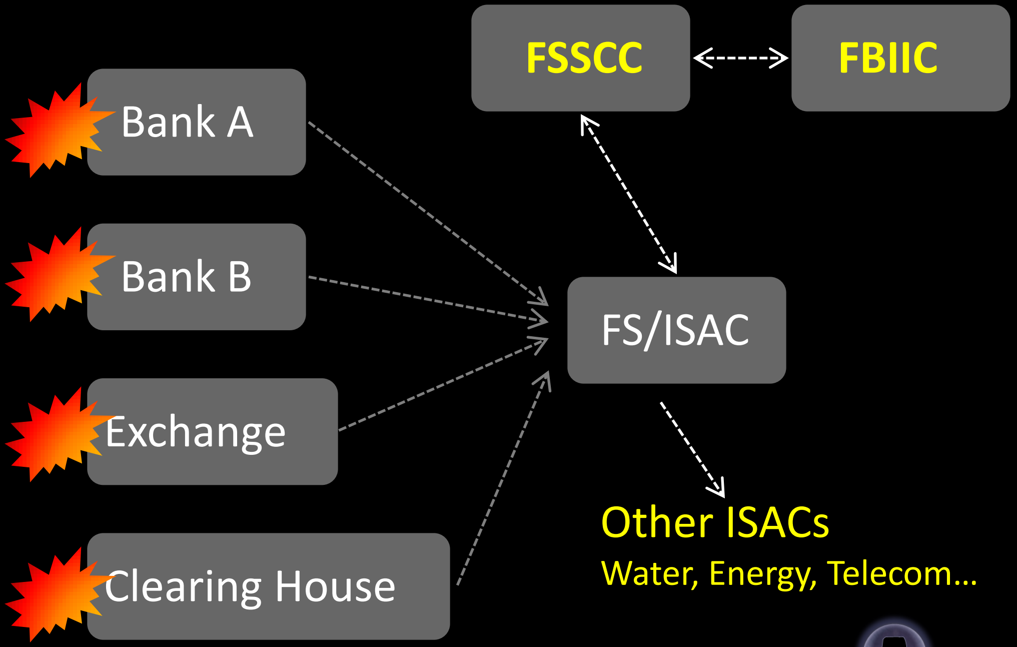
USSS

Then Share within the Sector



- *Operational* sharing and crisis management
- Shared with *all* financial institutions
- Sector-wide incident response via audioconfernce ‘bridge’ line
- Typically heard:
  - “What’s the vulnerability?”
  - “Is there a patch?”
  - What IP addresses?
  - “What works to mitigate?

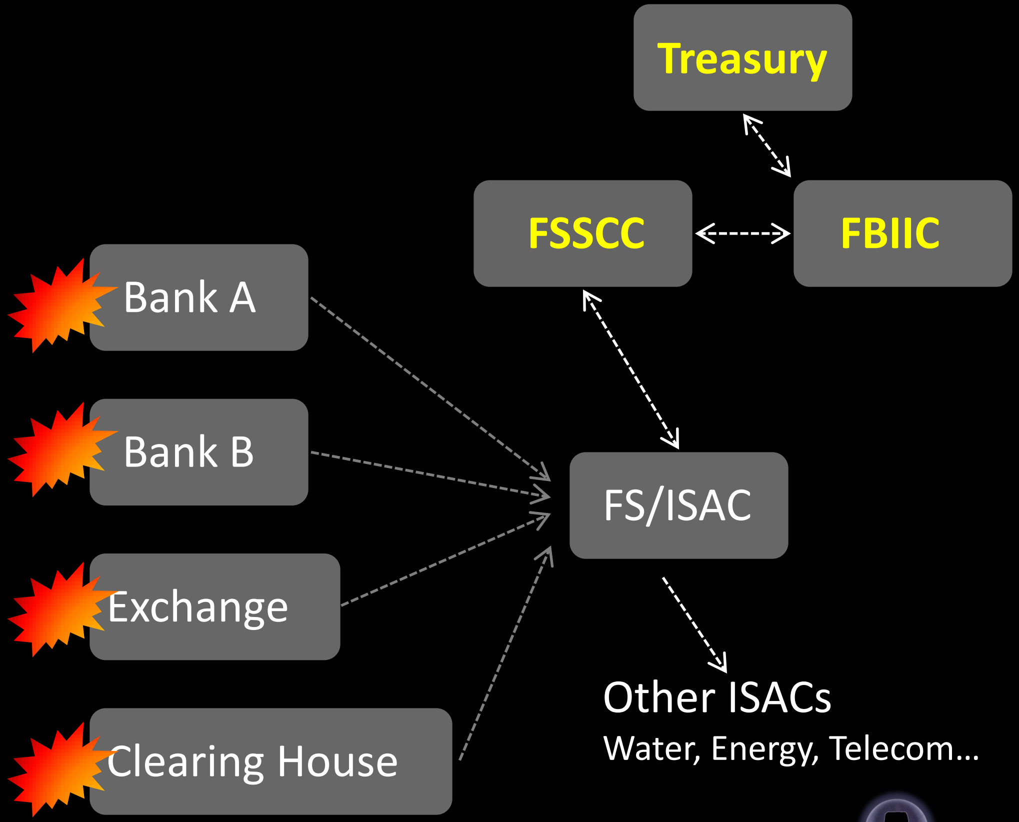
When More than Tech Discussions Are Needed…



Policy-Level Incident Response

- Senior company and government executives across all sector and regulators
- Management response via audio bridge
- Typically heard:
- “How healthy is the sector?”
- “What do we do if it gets worse?”
- “Can markets open as normal tomorrow?”

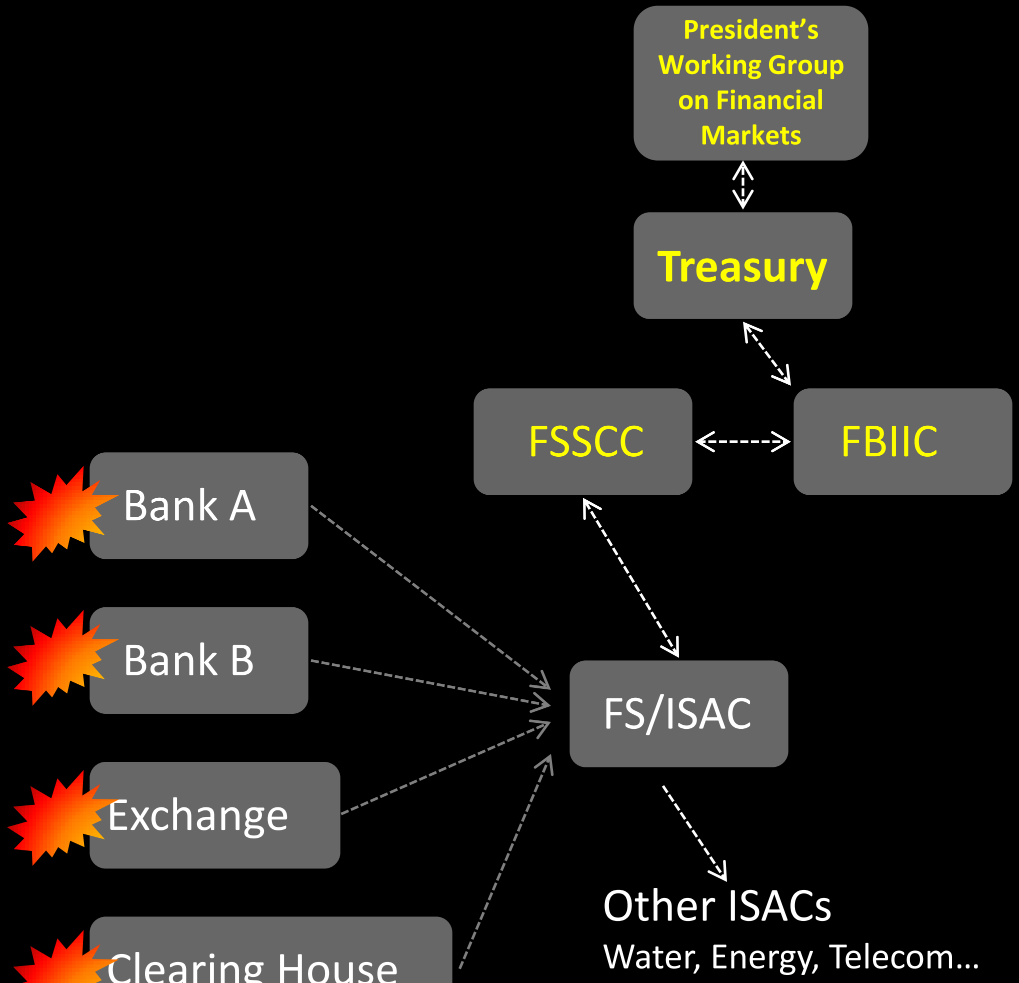
If Markets are Melting…



Within Treasury

- Escalate to the senior leadership, especially political appointees

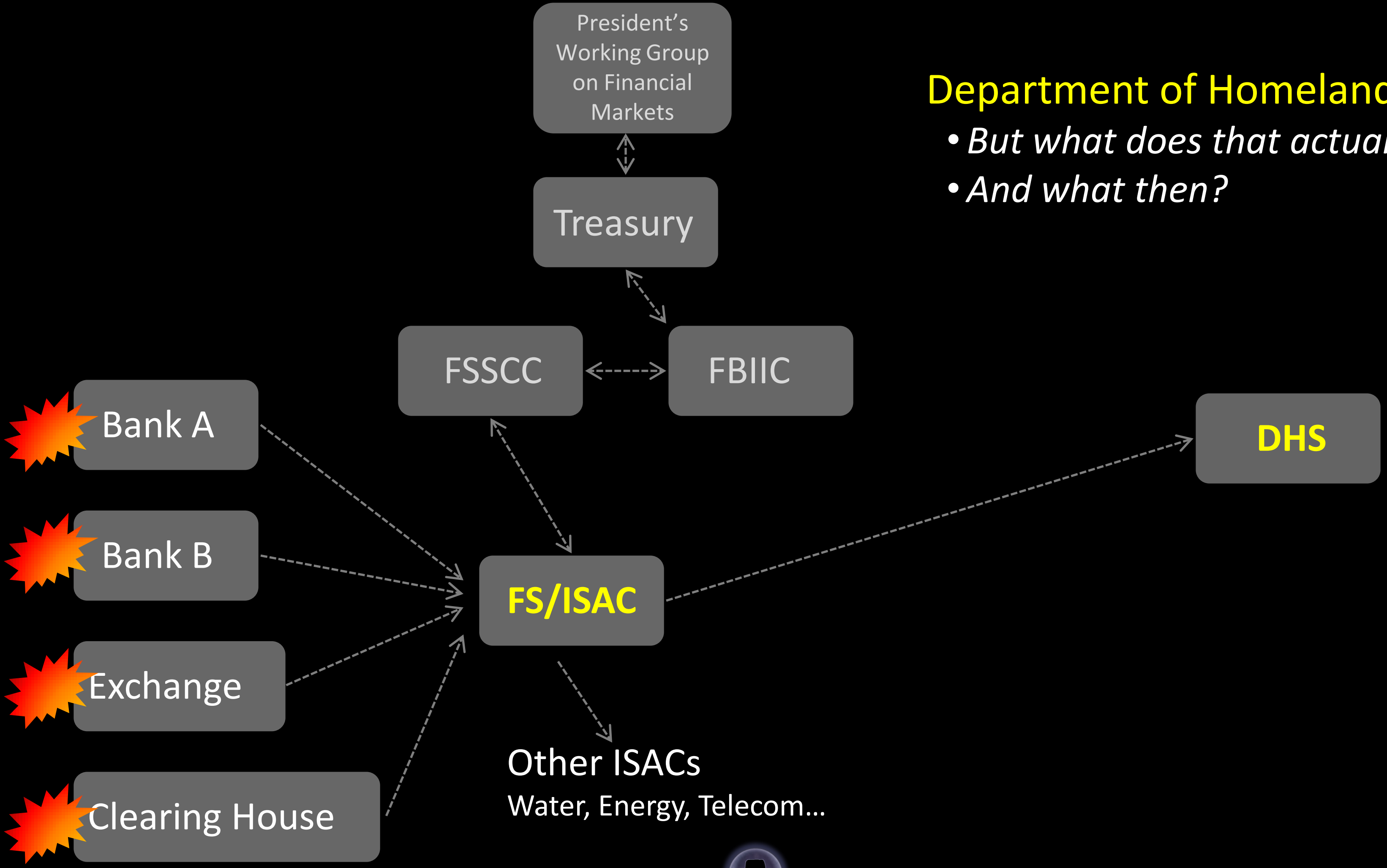
If Markets are Melting…



Highest Level of Financial Decision-making

- *No different than any other financial crisis!*
- *Secretary, Chairs of FRB, SEC, CFTC*

The *Cyber* Response…



President's Working Group on Financial Markets

Treasury

FSSCC

FBIIC

Bank A

Bank B

Exchange

Clearing House

FS/ISAC

DHS

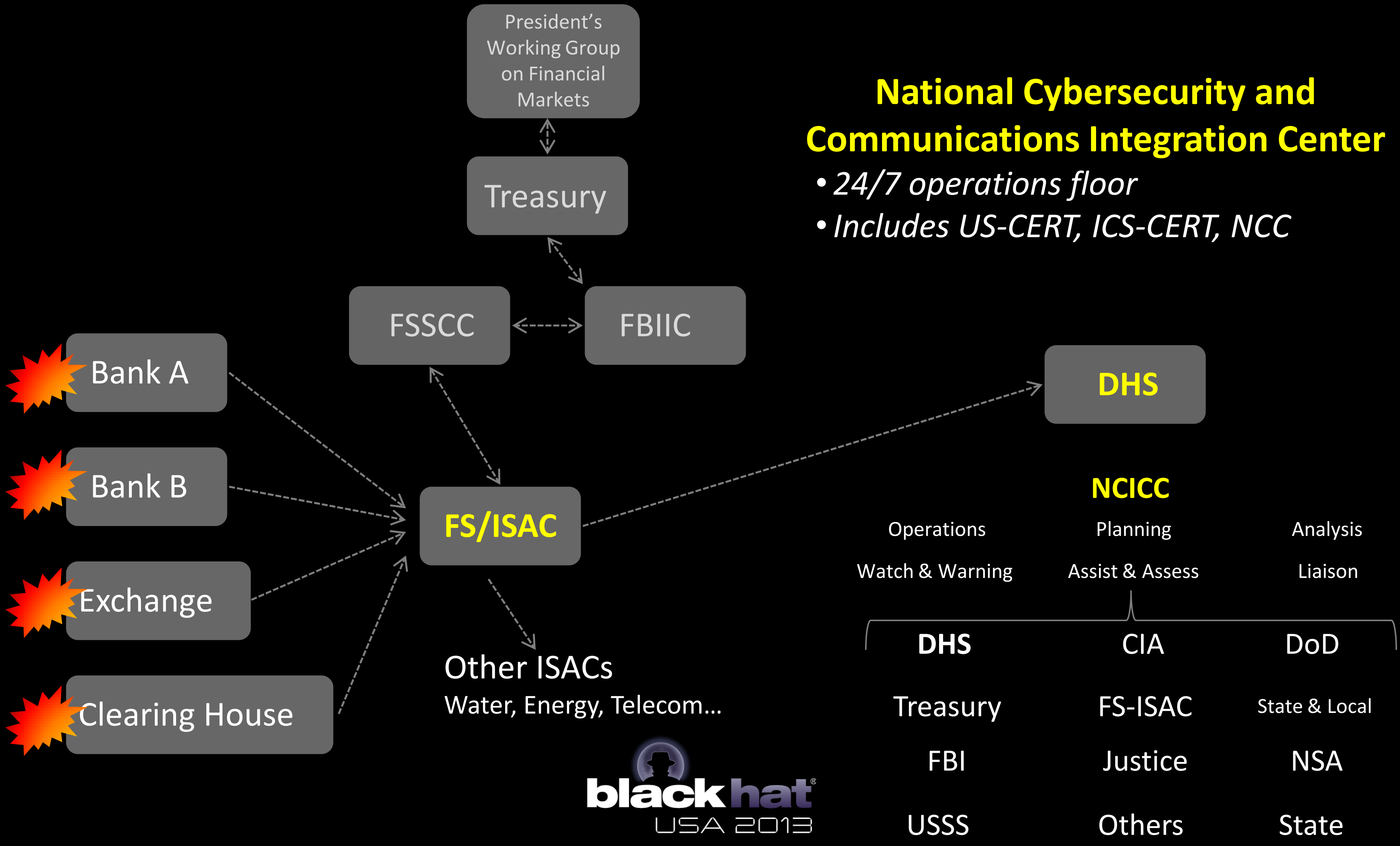
Other ISACs

Water, Energy, Telecom…

Department of Homeland Security

- *But what does that actually mean?*
- *And what then?*

The Cyber Response…



President's Working Group on Financial Markets

Treasury

FSSCC

FBIIC

Bank A

Bank B

Exchange

Clearing House

FS/ISAC

Other ISACs
Water, Energy, Telecom…

DHS

National Cybersecurity and Communications Integration Center

- *24/7 operations floor*
- *Includes US-CERT, ICS-CERT, NCC*

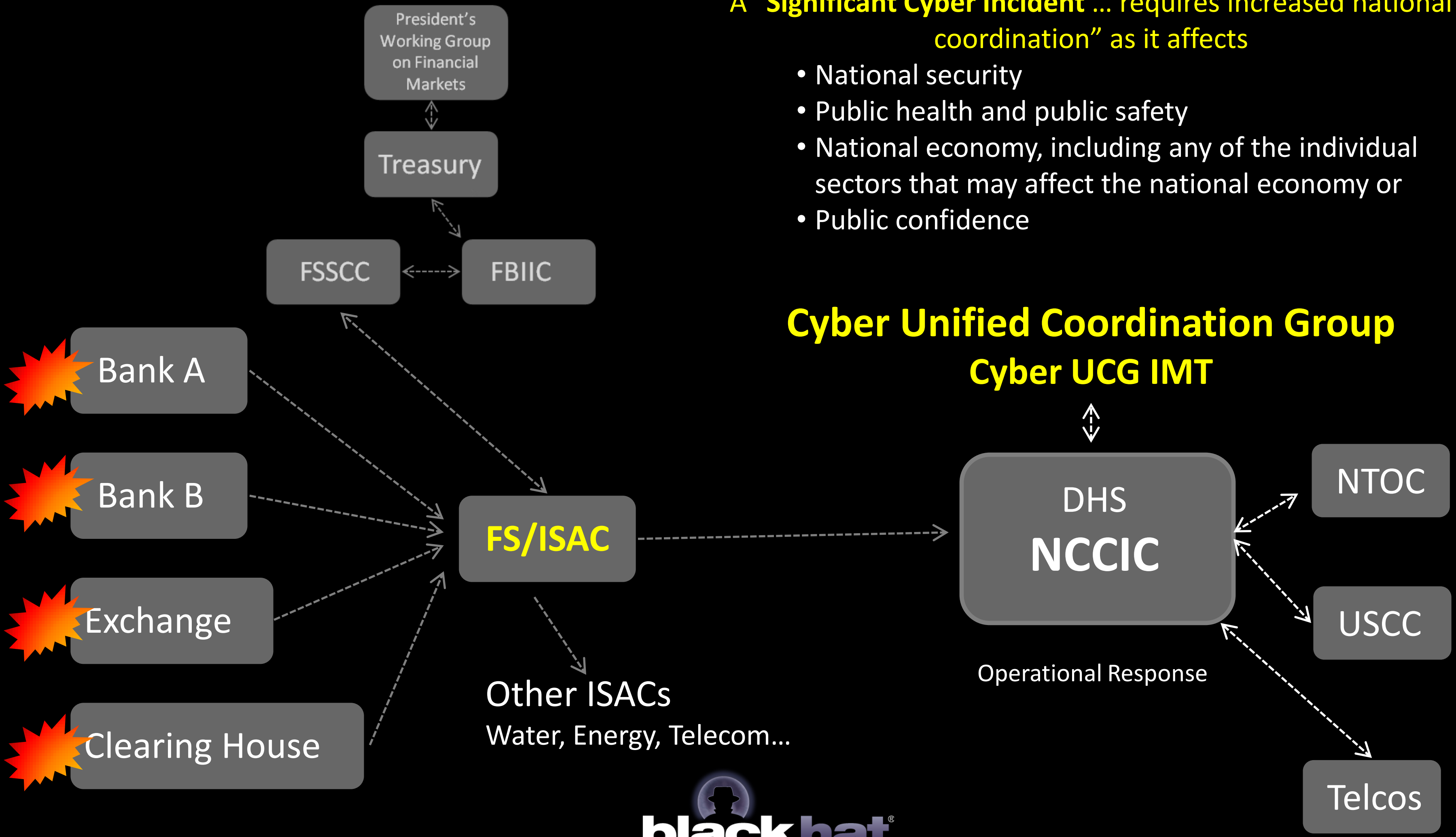
NCICC

Operations	Planning	Analysis
Watch & Warning	Assist & Assess	Liaison
DHS	CIA	DoD
Treasury	FS-ISAC	State & Local
FBI	Justice	NSA
USSS	Others	State

If Incident Needs Escalation

A "**Significant Cyber Incident** … requires increased national coordination" as it affects

- National security
- Public health and public safety
- National economy, including any of the individual sectors that may affect the national economy or
- Public confidence

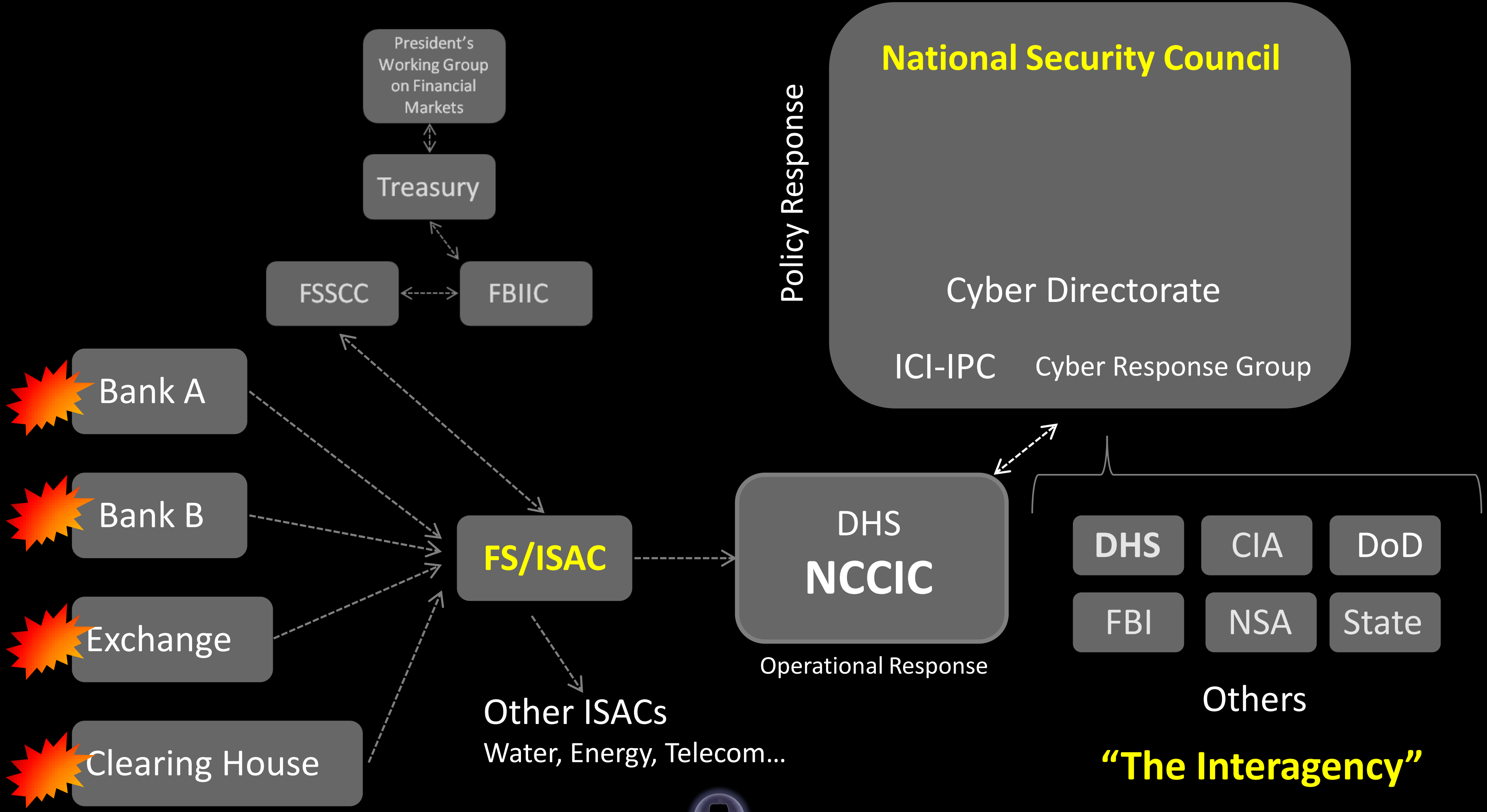


Who Coordinates Above DHS?

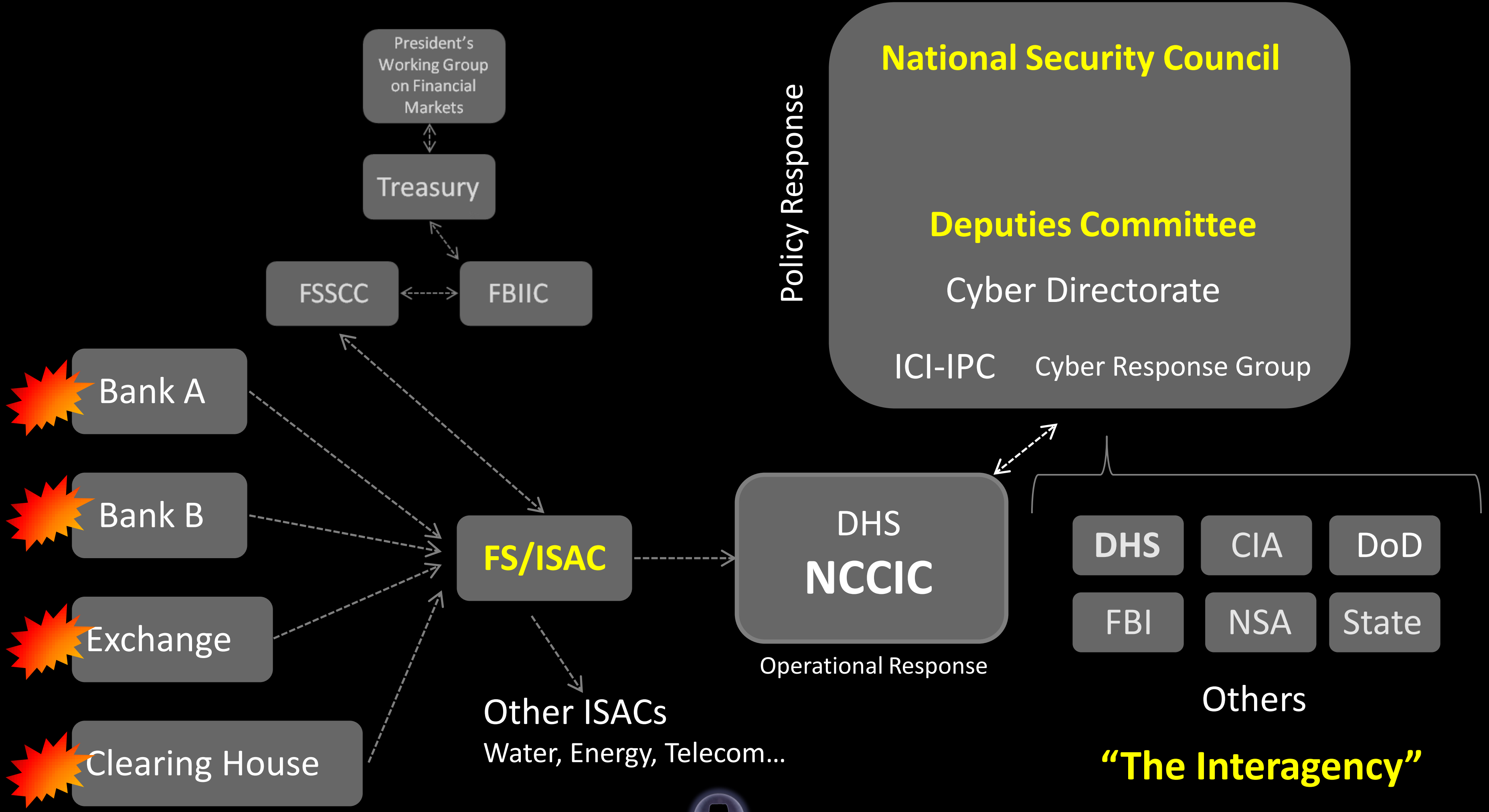
Who Coordinates Above DHS?

Who Coordinates Above DHS?

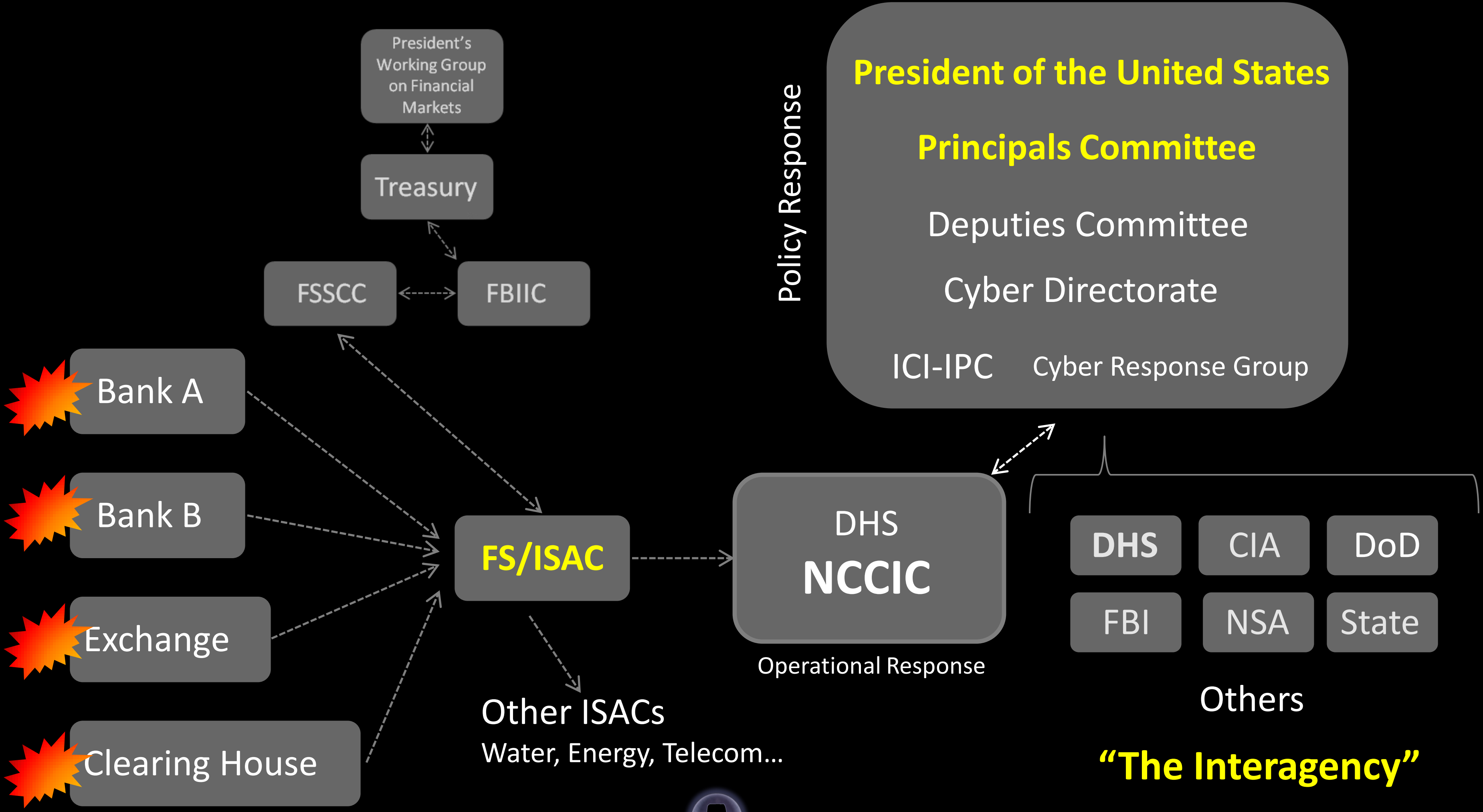
If Incident Needs Escalation



If Incident Needs Escalation



If Incident Needs Escalation



blackhat USA 2013

Why This Works

- Since
  - Worst-impact cyber conflicts generally caused by nations, not individuals and
  - Cyber conflicts tend not to be "network speed"
- Process translates "cyber crisis" out of technical channels
- Into the time-tested traditional national security crisis management
- Countries with NSC equivalents have natural edge to those without … like China

Why This is a Good Thing:

Provides Process for Tough Decisions

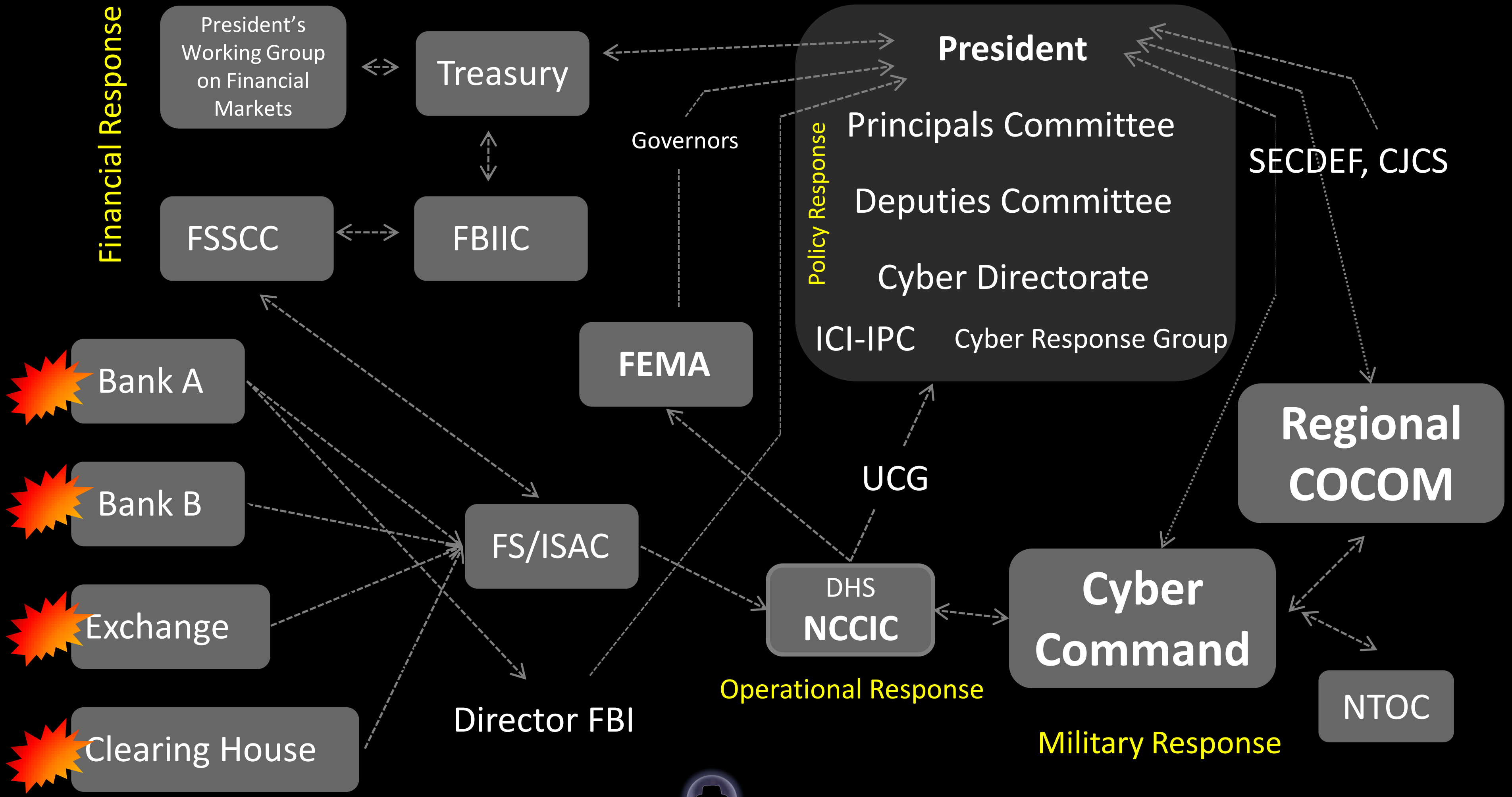
- Enables national-level technical response options
- Commitment of additional resources to help private sector response
  - Money, personnel, intelligence
- Determine "*what nation is responsible?*"
- Enables response using levers of national power:
  - Diplomatic, economic and yes, military

Why the Process Might Not Work or Otherwise Suck:

- It doesn’t always work even for physical crises!
- When government wants to control the response
- The “Katrina” of something on the edges of the system
- The “Six-Day War”
- True Cyber War

Why the Process Might Not Work:

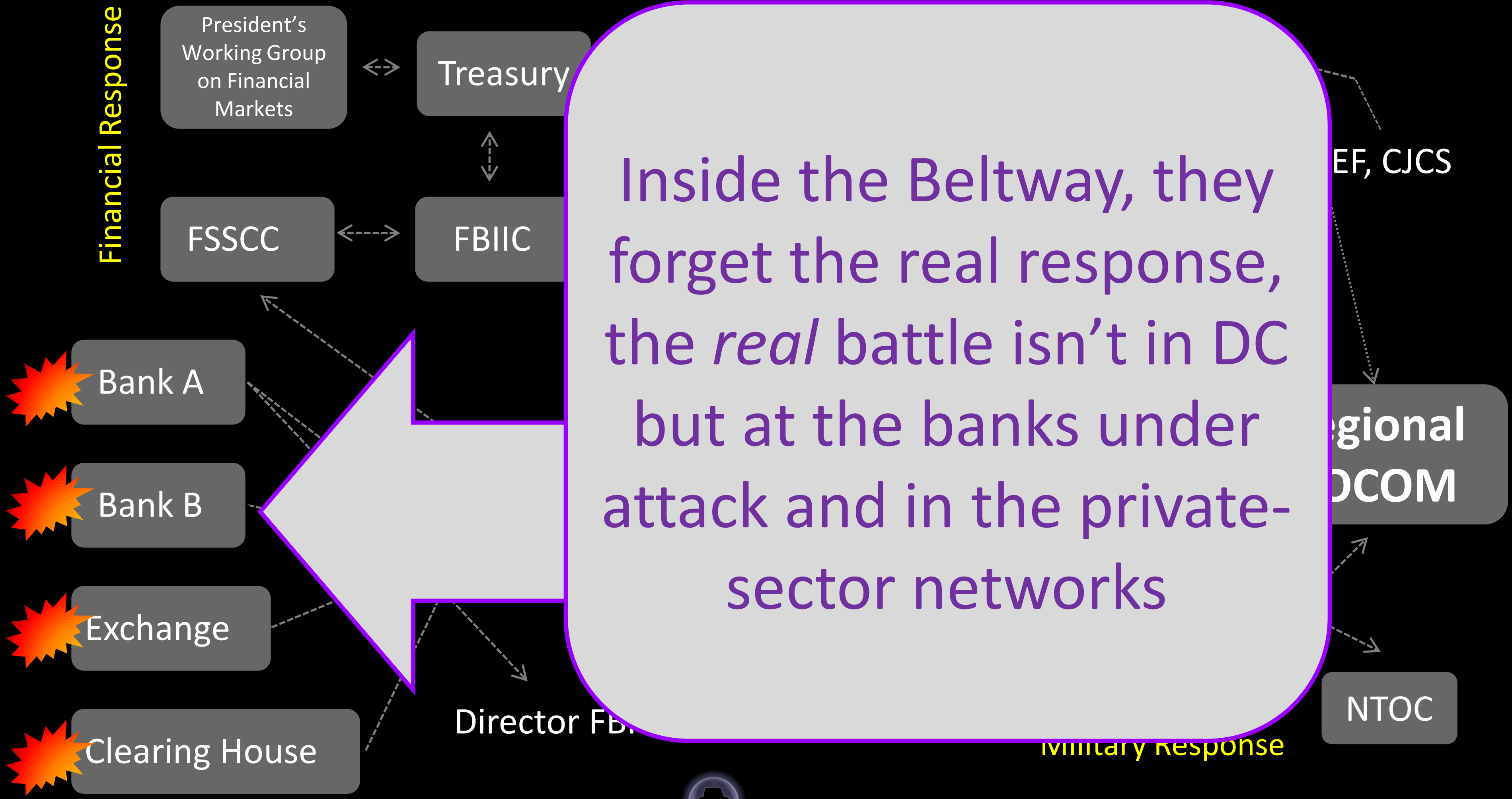
If We Are At Cyberwar!



black hat USA 2013

Why the Process Might Not Work:

If We Get Stupid…

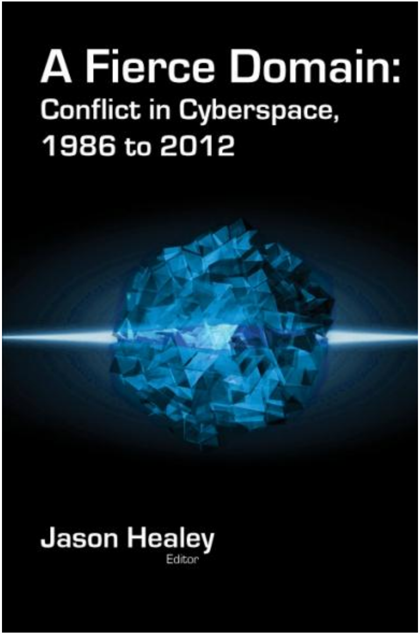


Inside the Beltway, they forget the real response, the *real* battle isn't in DC but at the banks under attack and in the private-sector networks

QUESTIONS?

Cyber Statecraft Initiative

- International conflict, competition and cooperation in cyberspace
- Publications (all at our website, acus.org)
- Public and Private Events



A Fierce Domain:
Conflict in Cyberspace, 1986 to 2012

Jason Healey
Editor

jhealey@acus.org Twitter: @Jason_Healey