
TALES OF INTEREST
Interesting (at least to me) selections from
BlackHat & Defcon 2013

Presenter

- Quinn R. Shamblin
  - Executive Director & Information Security Officer, Boston University
  - CISM, CISSP, ITIL
    (previously PMP, GIAC Certified Forensic Analyst)
  - qrs@bu.edu
  - 617-358-6310

BOSTON UNIVERSITY

Agenda

- The Washington view of cyber threats & the role of government in the incident response
- The NSA and PRISM
- IR from us to the President
- Sockstress DDoS
- The SpamHaus DDoS was easy (one person)
- MDM solutions under attack
- Creepy DOL

BOSTON UNIVERSITY

The Washington view of cyber threats & the role of government in the incident response

BOSTON UNIVERSITY

What is the level of the cyber threat?

- Ambassador Joseph DeTrani [8/2/2013 Defcon]
  - President of the Intelligence and National Security Alliance (INSA).
  - Prior:
    - Senior Advisor to the Director of National Intelligence
    - Director of the National Counter Proliferation Center
    - National Intelligence Manager for Counter Proliferation
    - North Korea Mission Manager for the ODNI
    - CIA

- The cyber threat is just as grave as other weapons of mass destruction, including…

Similar level, but different character

- If you take out an entire sector,
  you could cripple an entire country
- Unlike the nuclear threat, MAD is not a factor
  - With nuclear one would be “mad” to use a nuclear attack. (Mutually Assured Destruction)
  - This is not necessarily true with cyber because of the problem of attribution
- This may make a cyber attack more attractive to an aggressor
- Ambassador DeTrani urges we look at this just as we did Nuclear, Chemical and Biological weapons after WWII
  - Treaties are needed

When I was Deputy Secretary of the DHS, one comment I heard all the time was, ‘Why isn’t the government doing something about this?’

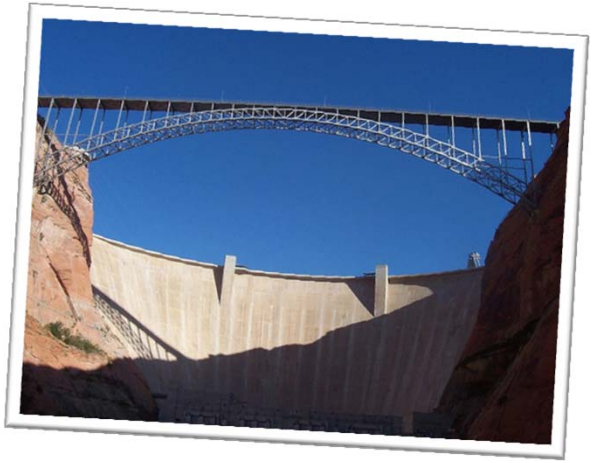
– Mark Rutherford

What is the government good at?

- What should we rely on them to help us with?
  (…and provide input to them on so they can do a better job)
  - Definitions and standards
  - Creating national policy
  - Passing laws to enable/control the response
  - Responding to a true national emergency
    - Bringing resources to bear
  - Funding research and innovation
  - Incentive programs
  - Establishing treaties

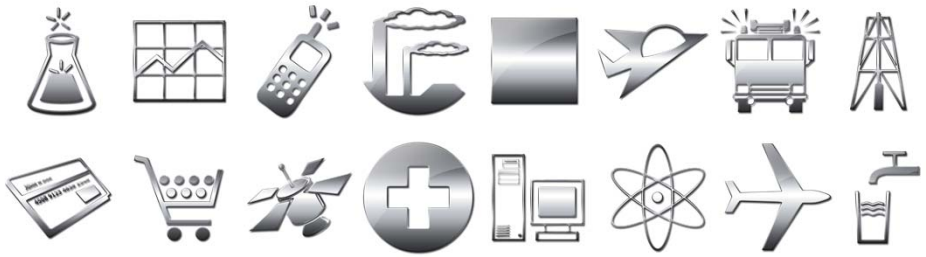
G+1: Definitions of standards

- Critical Infrastructure
  - What is truly important: The backbone of the U.S. economy, security and health
  - Security: Reducing the risk to critical infrastructure by physical means or defense cyber measures to intrusions, attacks, or the effects of natural or man made disasters
  - Resilience: The ability to prepare for and adapt to changing conditions, and withstand and recover rapidly from disruptions.
- NIST
- DHS



G+1: Critical Infrastructure Sectors

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy



- Financial Services
- Food and Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- Nuclear Reactors, Materials, and Waste
- Transportation Systems
- Water and Wastewater Systems

G+2: Creating National Policy

- How are cyber crimes to be treated and classified?
- What is the policy position with respect to harmful acts committed using cyber technology?
  - “We don’t negotiate with terrorists”

BOSTON UNIVERSITY

G+3: Passing Laws

- Facilitate & enable response
  - Surveillance / Prism
- Incorporate appropriate control and oversight
- Balance
  - National
  - Business interests
  - Personal interests
  - Privacy concerns

BOSTON UNIVERSITY

Laws related to information security

- Constitution [Bill of Rights (4th Amendment)]
- Wiretap Act [18 USC 2511(2)(a)(i)]
- Electronic Communications Privacy Act [18 USC 2701]
- Computer Fraud and Abuse Act [18 USC 1030]
- Economic Espionage Act [18 USC 1831-39]
- Child pornography [18 USC 2252]
- Criminal copyright [18 USC 2319 and 17 USC 506]
- Criminal trademark [18 USC 2320]
- Criminal trade secrets [18 USC 1831, 1832]
- Threats and harassment [18 USC 844 and 875, 47 USC 3a1(C,E)]
- Reckless conduct [18 USC 1030(a)(5)(A)(ii)]
- Lanhum Act [15 USC 1051]
- FISA 201 and 730 (“PRISM”) [36 USC 1801]
- U.S.A. P.A.T.R.I.O.T. Act

Similar laws in other countries

- Most democratic countries have similar laws and have had for a long time…
- EU Data Privacy
  - Article 2. Unauthorized access to information systems
  - Article 3. Systems interference the
  - Article 4. Data into parents
  - Article 5. Instigation, eating and abetting and attempt
- UK Computer misuse act of 1990,
  - Section 1 access to Computer Materials
  - Section 2 access with intent to commit a facilitate the mission of further offenses
  - Section 3 modification of computer material
- Germany criminal code
  - section 202a spying out data
  - section 303a modification of data
  - section 303b computer sabotage
  - section 263a computer fraud

G+4: National Emergency Response

- …Katrina aside…
- True national emergency or crisis with impact across an entire sector or multiple sectors
- (We will go over this in detail in another section)
- ISACs - information sharing and analysis centers
  - One for each sector of critical infrastructure

BOSTON UNIVERSITY

G+5: Funding supporting activities

- Funding research and innovation
  - Startups, Self sustaining , Darwinian
- Creating incentive programs
- Positive social engineering

BOSTON UNIVERSITY

G+6: Establishing treaties

- Encourage the use of the peaceful use of cyber capabilities while deterring harmful ones
  - As we attempt to do with nuclear, chemical and biological technology
- Collection of information in a way that is acceptable to International partners
- International threat intelligence information sharing
- International law enforcement cooperation
  - Law enforcement action facilitation

BOSTON UNIVERSITY

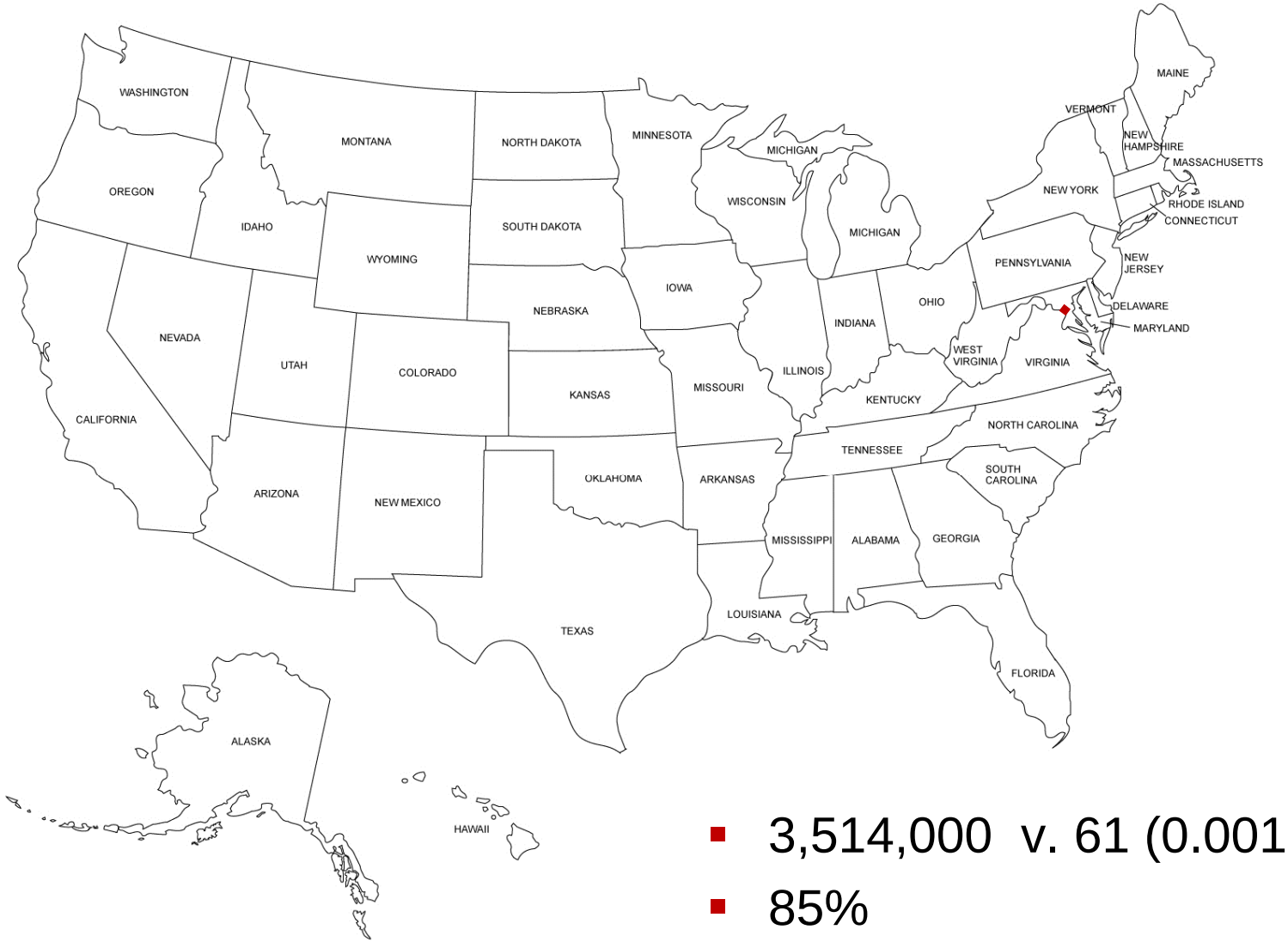
What is the government *not* as good at?

…Even if they think they are

- Knowing our businesses and what we need
- Providing unique actionable information
- Innovation
- *Solving* the problem of cyber security

BOSTON UNIVERSITY

G-1: Knowing *our* business



- 3,514,000 v. 61 (0.00174%)
- 85%

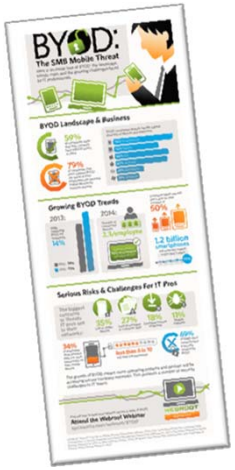
G-2: Providing actionable intelligence

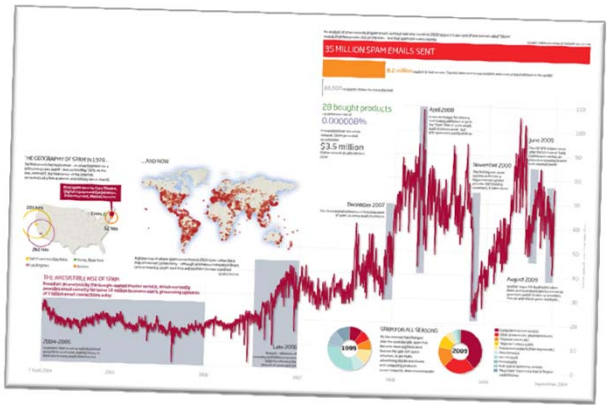
- 4%
- The problem of classification (over-classification)
  - The same thing you saw on CNN
- Does the government have a greater intelligence gathering capability than the private sector?
  - The answer depends

BOSTON UNIVERSITY

G-2: Providing actionable intelligence

- Intelligence/threat information provided by industry
  - High quality global threat reports: Verizon, Symantec and McAfee
  - Targeted reports on specific threats
- Automated global threat reporting networks





G-3: Innovation

- Drags on the system
  - Unavoidable necessity of approvals
  - Risk averse lawyers
  - Classification of information
- Private sector innovation
  - Pace of growth
  - Darwin

BOSTON UNIVERSITY


Darwin Award in
3… 2… 1…

G-4: Solving the problem for us

- Government it is in its own way
- Cannot share information with some who should really have it

BOSTON UNIVERSITY

Bottom line

- The government is not going to solve this for us

- We largely have to help ourselves
- We can encourage the government to continue doing things that it is good at doing…

BOSTON UNIVERSITY

…Such as: (Things government is good at)

- Continue to develop intelligence, but…
  - Work to get it into the hands of industry more quickly
  - Revise data classification schemes as they apply to the threat sharing information
- Work with industry to establish a single standard for threat sharing information exchange format.
  - Consider elements of the format that will allow for rapid declassification of threat data
- Facilitate large scale/regional level/national level/incident response exercises
- Fund supporting activities…

More things government is good at

- Provide funding
  - For research and development
    - Facilitate transfer of technology to the private sector
  - Incentives / funding structures for startups
    - 90% will fail. 10% will lead innovation
  - Incentives / funding to grow & maturity the ISACs
  - Fund / incentivize training…

More things government is good at

- Incentivized training (Examples of how + pramid)
  - Behavior and knowledge training/positive social engineering in primary and secondary school
  - Sponsored education and training tools
    - Quality compelling content available to all
  - Higher education skills training programs
    - Not enough talent out there right now
  - Workforce training programs
    - Compliance tried to funding/grants

What do we need to do for ourselves?

- Establish or join communities of trust.
  - Open the lines of communication
  - Work amongst ourselves to share threat information.
- Where possible within some other organizations, establish a row on the insider threat programs
- Demand better from our vendors.
  - Work through our industry ISACs to put pressure on the vendors [Long standing BCP38 issue]
- Train our people

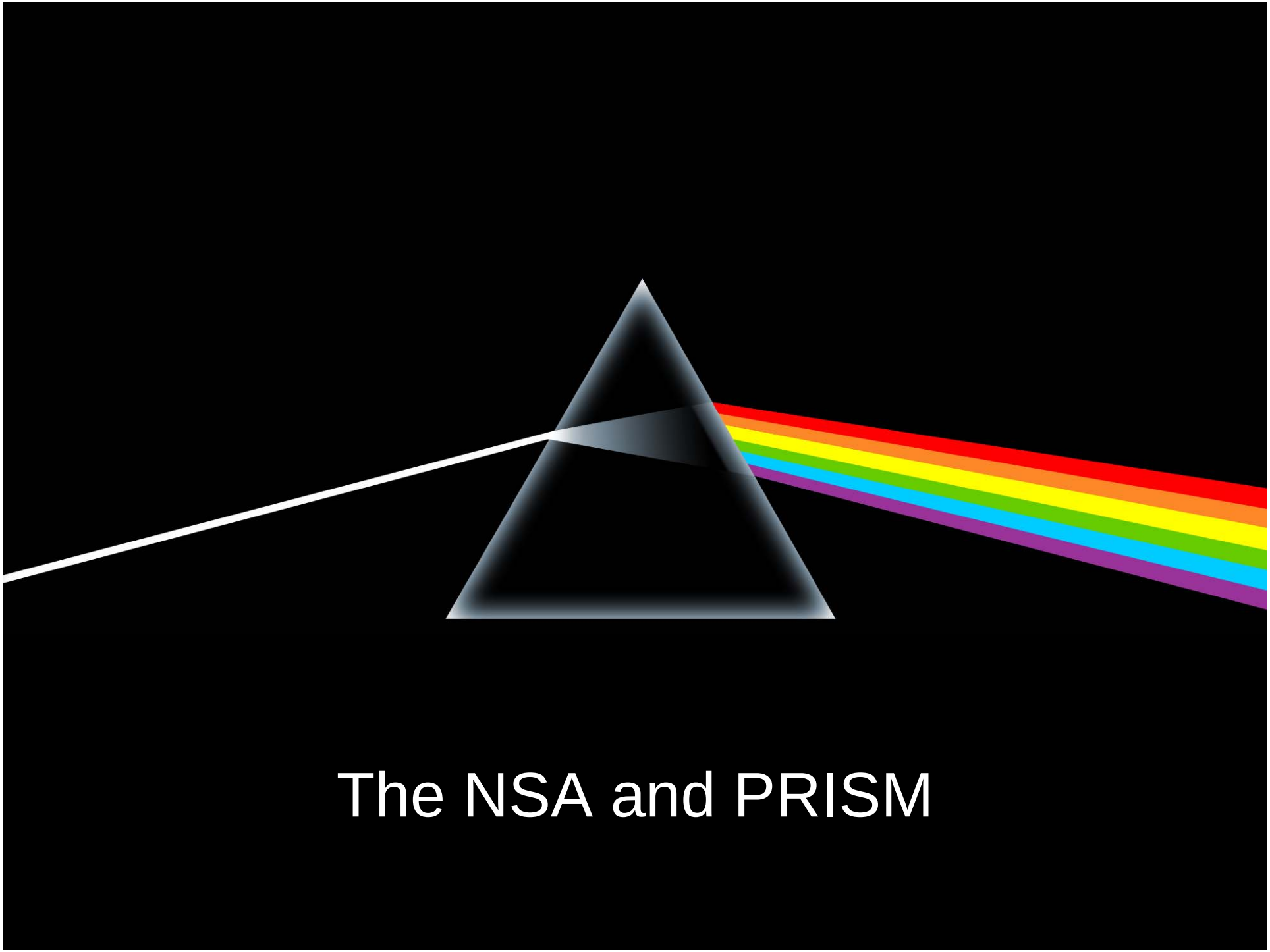
Training

- Blackhat - help wanted signs
  - If you have skills in this field, you can get a job
- Not enough people
- Impacts both government and industry
  - Impacts the government more
- Continue your training, get your people trained
  - Build from the ground up

Strategic Leaders – Visionaries that advance the mission

Operational Leaders – Integrate technical skills with the mission

Functional (Technical) Leaders – Technical subject matter experts



The NSA and PRISM

General Keith Alexander at Blackhat

Foreign Intelligence Surveillance Act

- Surveillance program started in 2007
  - Provided avenue through Wiretap Act & ECPA
  - Permitted for counterterrorism purposes only
- Two levels
  - Section 215 authority, business records
  - Section 702 authority, content of communications
- What the NSA is doing is legal
  - Virtually every democratic country has laws allowing for legal intercept
  - “Model of oversight”

Section 215 authority

- "Business records" – Metadata program to connect dots "in the least intrusive way possible"

- Telephone meta data only
  - Date/time of call
  - Calling number
  - Receiving number
  - Duration of call
  - Source of the above data

- no voice communication
- no SMS text messages
- no subscriber information
- no names
- no addresses
- no credit card numbers
- no location information

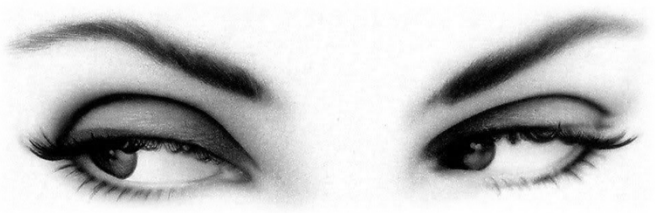
Access and authorization

- Industry is compelled by the court to comply
- Section 215. U.S. call records metadata database
  - Only 35 people at the NSA can run queries
  - Only 22 can approve that a query be run
  - Only 300 numbers were approved last year
  - Only 12 reports were provided to the FBI
  - Those reports contained less than 500 numbers
- This is all the NSA has, for content, go to the FBI

Section 702 authority

- Lawful intercept of communications content of foreign persons.
- The intent is to find the terrorist that walks among us.

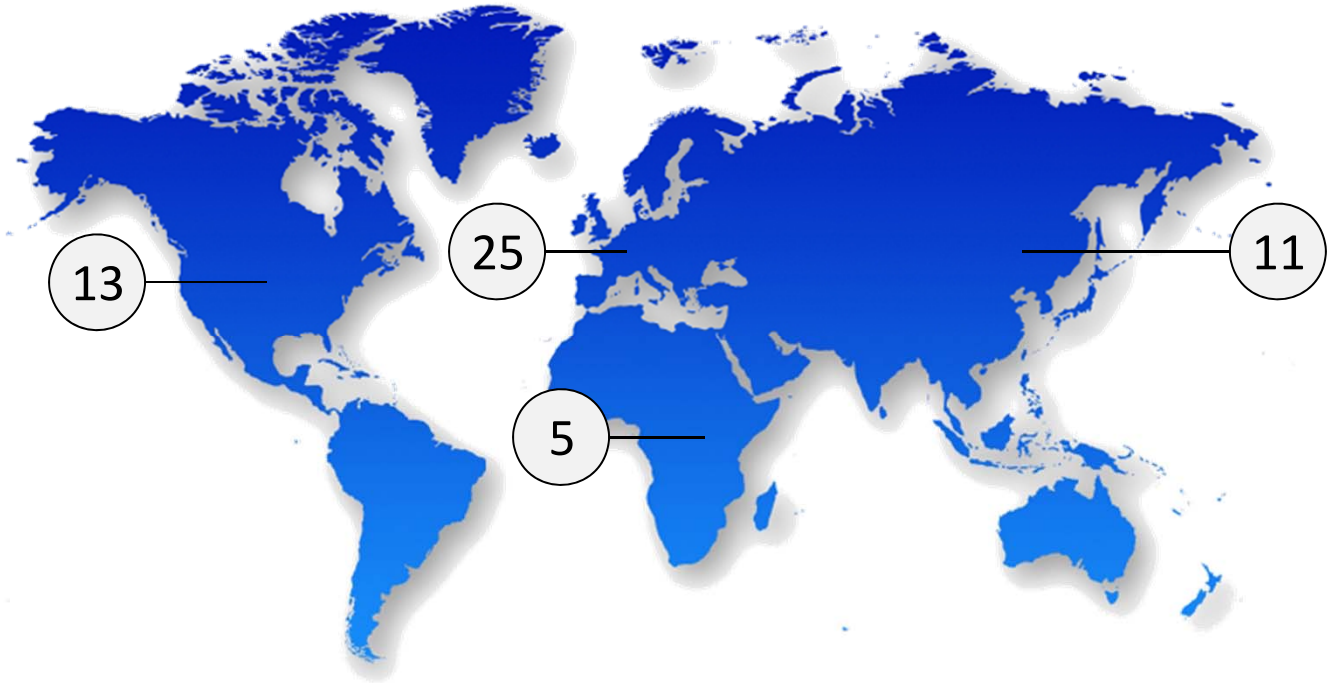
Oversight



- Representatives from all three branches of government must agree
  - Federal circuit court judges oversee approvals
  - Congress reviews all actions
  - Administration oversees
- Internal NSA activity monitoring
  - NSA audits 100%of the activity of their employees.
  - 100% auditability on ever query made.
    - Audited by inspector general.
  - The NSA has a directorate of compliance.
    - White house. Intel committees of congress. AG.

Program results

- These tools have stopped 54 terrorist-related activities since 2007



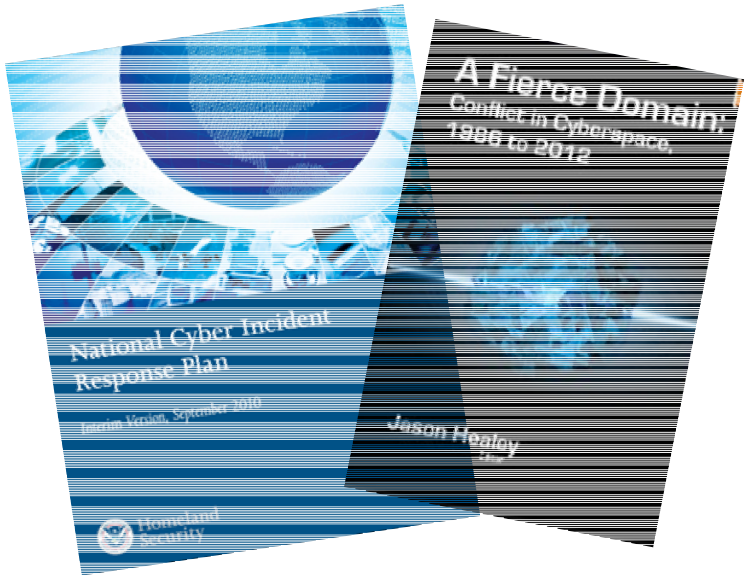
- This is a partnership a between us and our allies.

IR …from us to the President

BOSTON UNIVERSITY

Incident Response

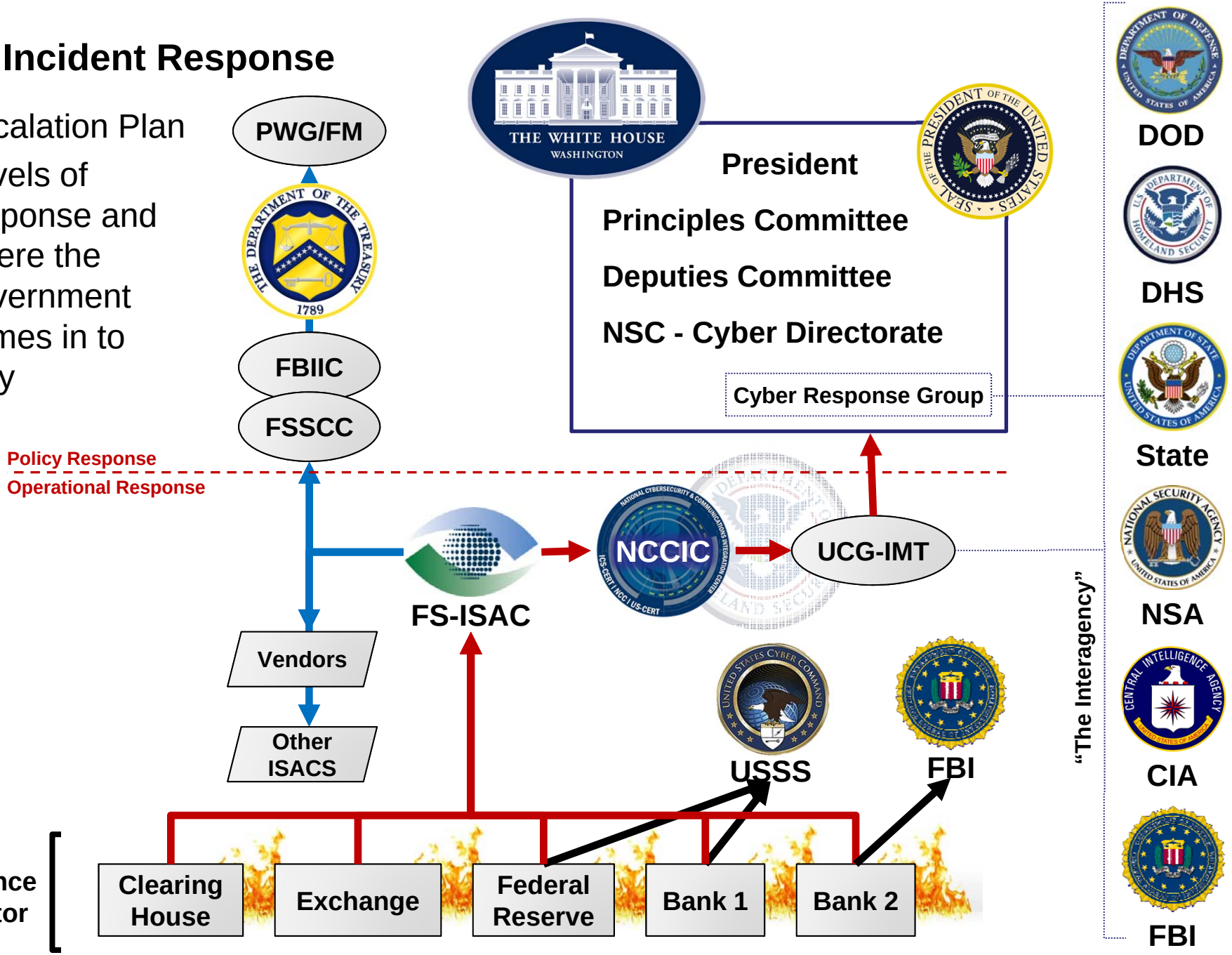
- Local Level
  - Find and fix the problem
  - Share with partners/colleagues/sector representatives
- National Level
  - National/International implications
    - Misunderstandings
    - Attribution
    - Policy-level decision making
    - Large-scale response



BOSTON UNIVERSITY

U.S. Incident Response

- Escalation Plan
- Levels of response and where the government comes in to play



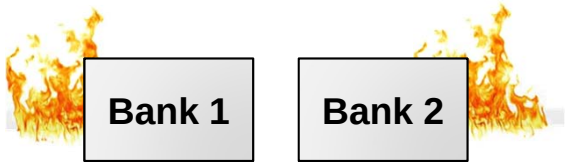
Finance Sector

- Important/large/central banks
- The Federal Reserve Bank
- Exchanges
- Clearing Houses

Large-scale attack on a firm

First Response

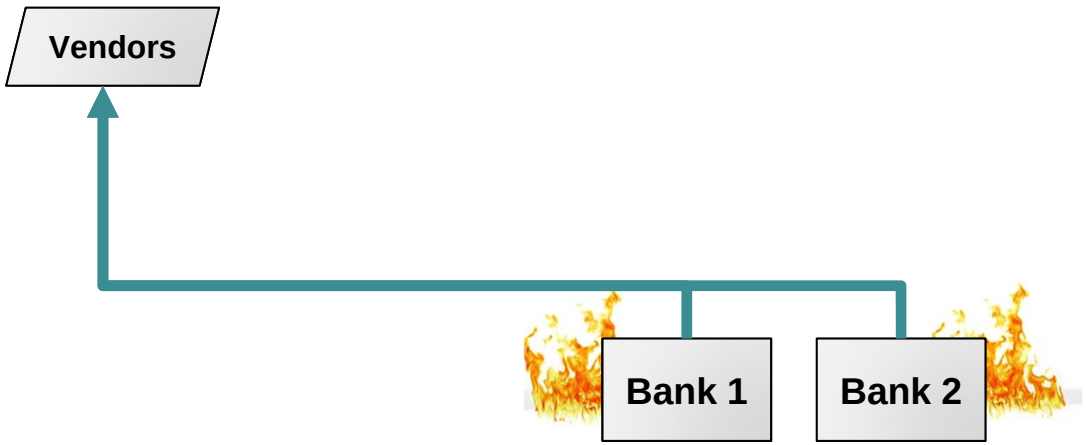
- Responders
  - Local Incident Response personnel
  - (Attorney?)
- Questions
  - What kind of attack? (purpose, subject)
  - How did they get in? (vector)
  - What tactical steps to stop or mitigate attack?
  - Can we restore service?
  - What evidence/artifacts can be preserved for future analysis/investigation/prosecution?
- Who will they call if they need help?
  - Trusted colleagues/partners
  - Other institutions
  - Beyond that….



Large-scale attack on a firm

First Escalation

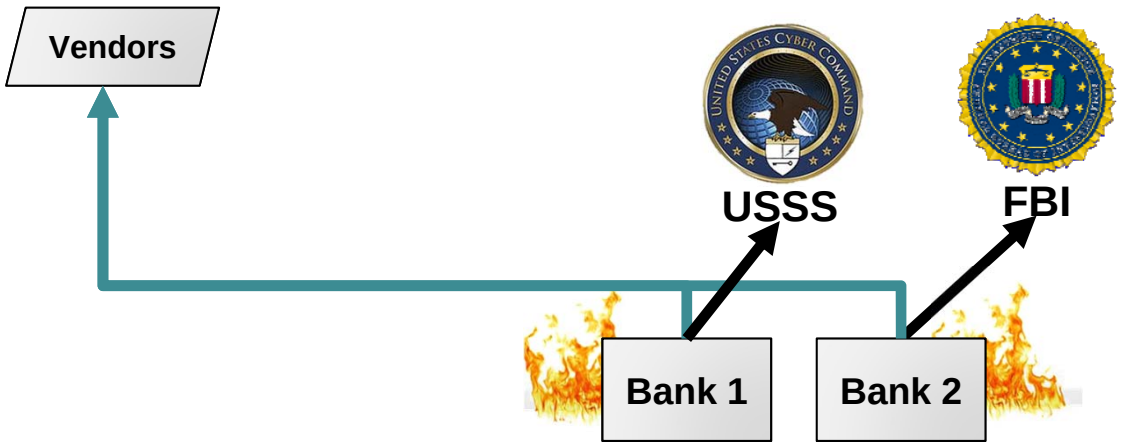
- Call in a Tiger Team / Technical Incident Response Firm



Large-scale attack on a firm

Escalation to
Law Enforcement

- Each institution will call the Federal Policing agency with whom they have the best relationship
- In the finance sector, typically the FBI or US Secret Service



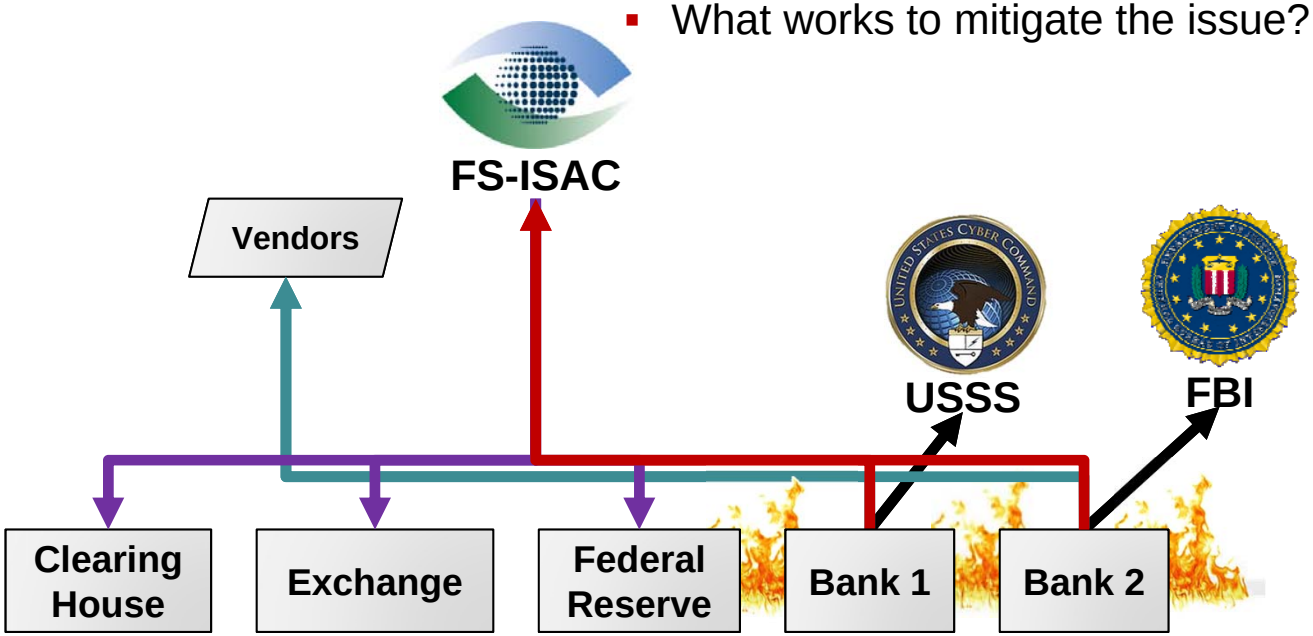
Large-scale attack on a firm

Information sharing with sector colleagues via the

Financial Sector

Information Sharing and Analysis Center (ISAC)

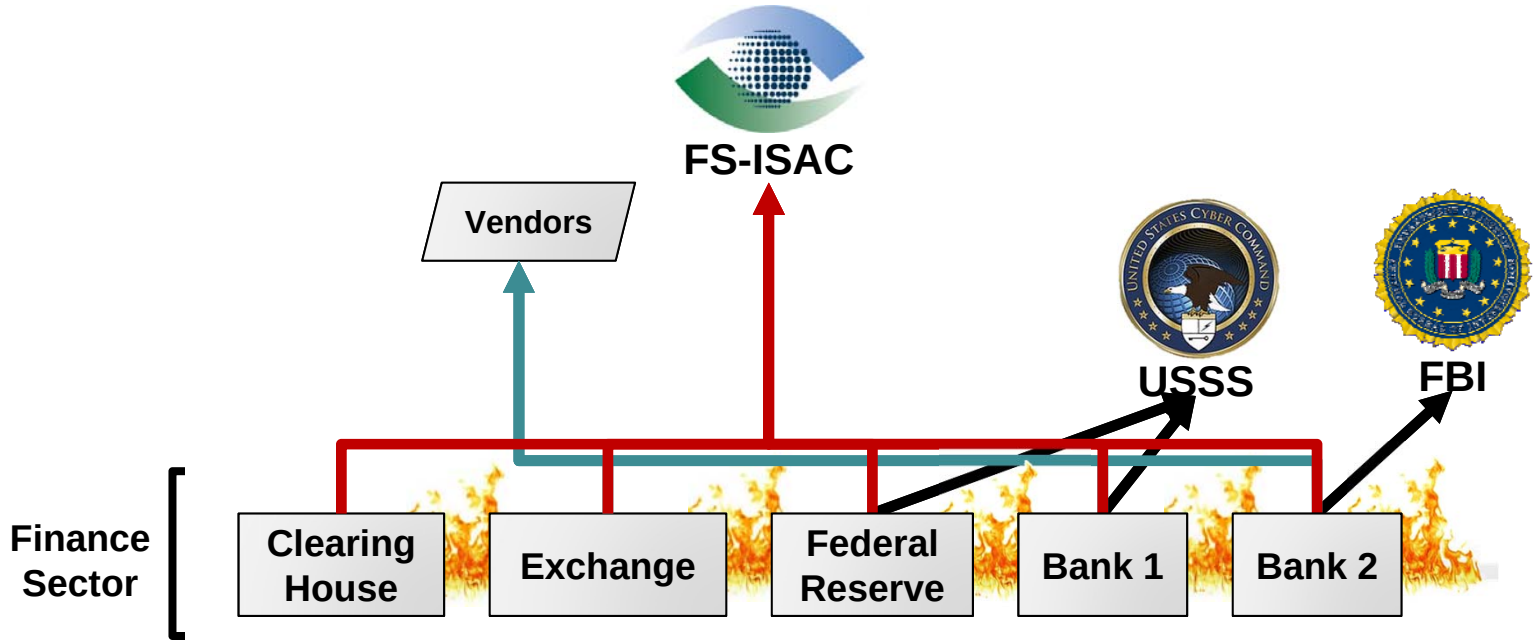
- They then share the threat information with their colleagues in their sector
  - (This step may be before or after contacting LE)
- Until this point, they don't know that the attack they are seeing is the same or related to one being seen by another bank
- Questions:
  - What is the vulnerability?
  - What is the largest attack you have seen?
  - Is there a patch?
  - What works to mitigate the issue?



Large-scale attack on the whole Sector

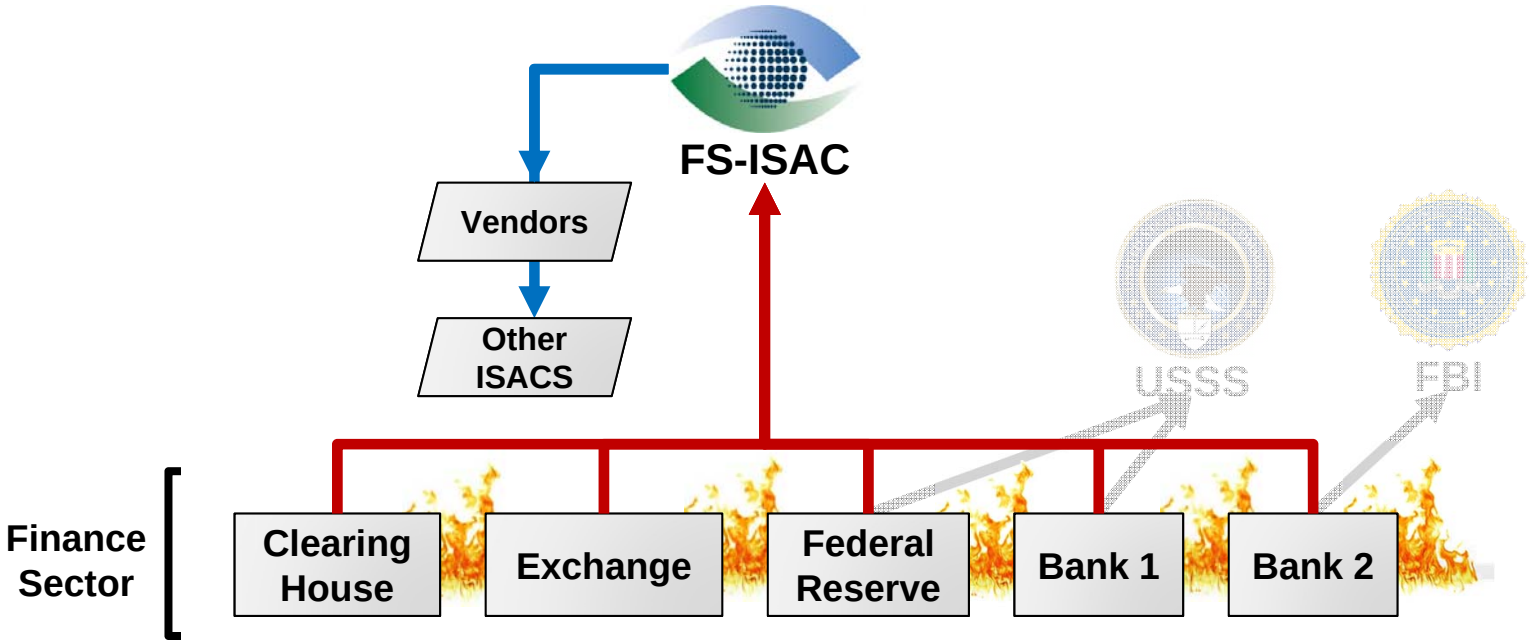
Follows the same path up to the Information Sharing and Analysis Center (ISAC)

- If the entire sector is under attack, each institution would follow the same basic process
- When the information gets to the sector's ISAC, the pieces are put together and they can see it is a sector-wide event
- Operational Response
  - Not anonymous
  - Share with all financial institutions
  - Community of trust



Expanded Scope & Leverage

- Collective pressure on the vendors
  - Drive greater responsiveness and focus
- Coordination information sharing with ISACs for other sectors
  - Defense Industrial Base
  - Telecomm
  - Energy
  - Water

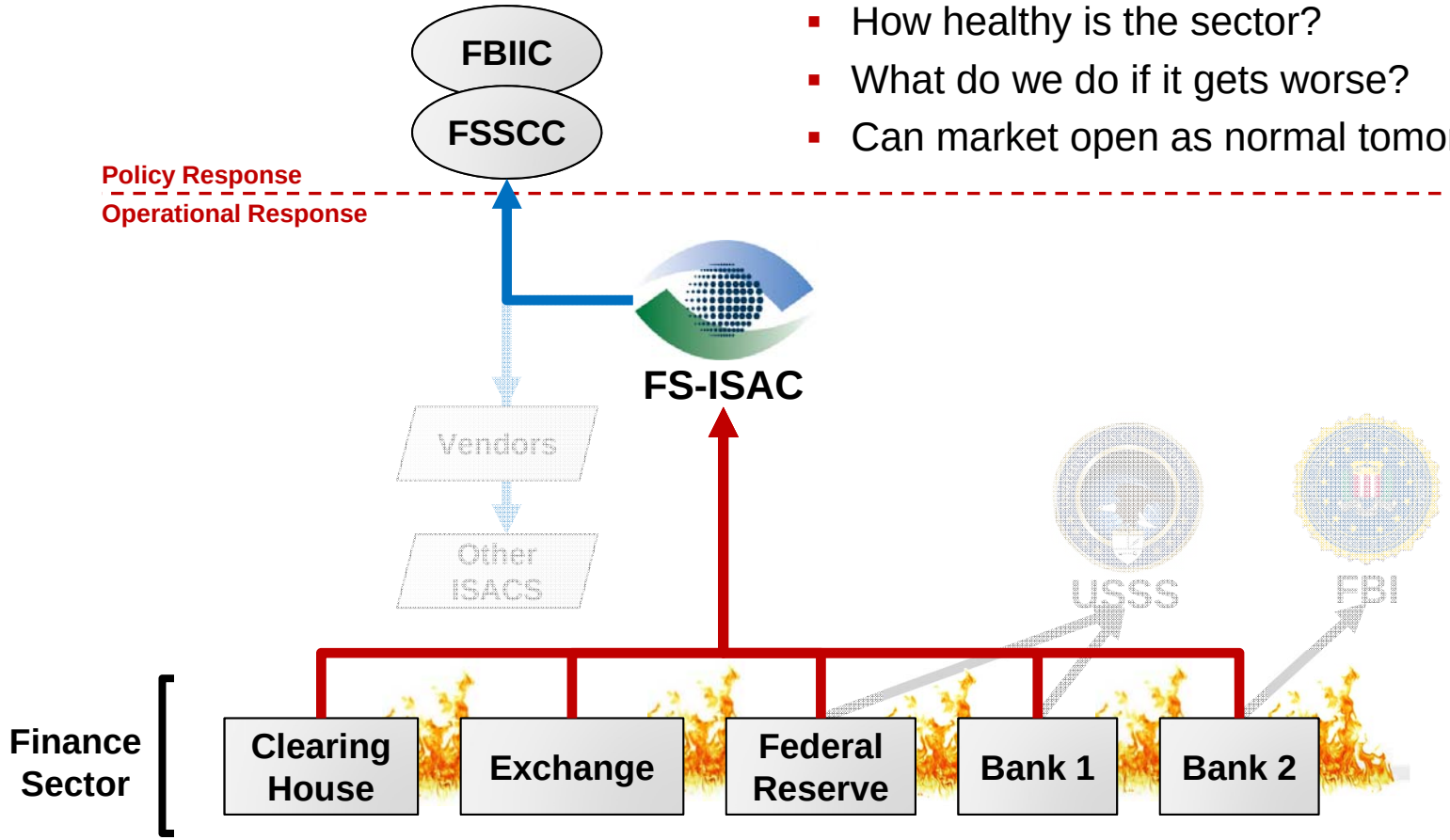


Beyond the Technical

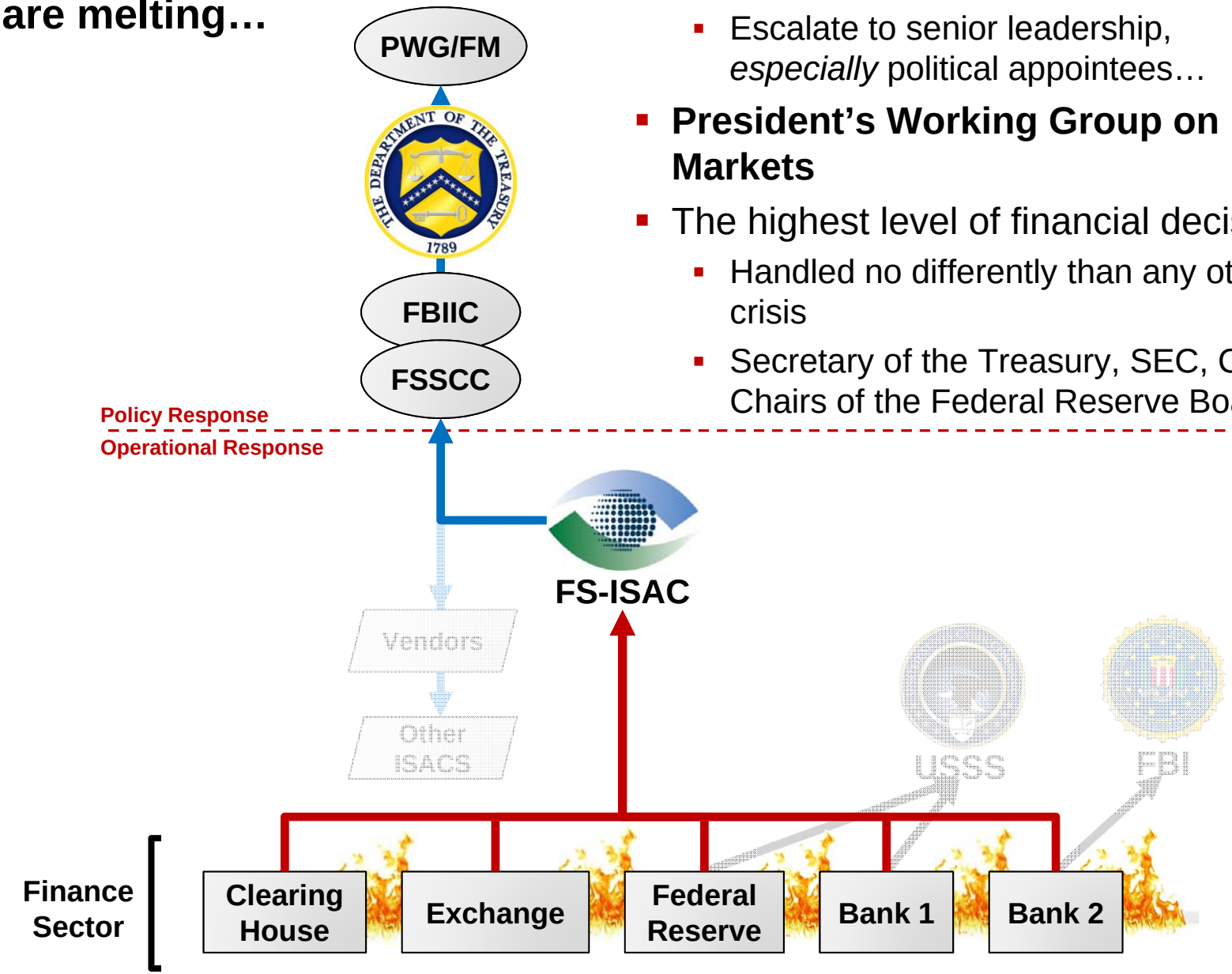
Financial Services Sector Coordinating Council (FSSCC)

Financial and Banking Information Infrastructure Committee (FBIIC)

- *Policy-Level* Incident Response within sector
- Sector-wide discussions at the highest levels
- Senior company and government executives and regulators
  - Can change rules/shift policy, if needed
- Questions
  - How healthy is the sector?
  - What do we do if it gets worse?
  - Can market open as normal tomorrow?



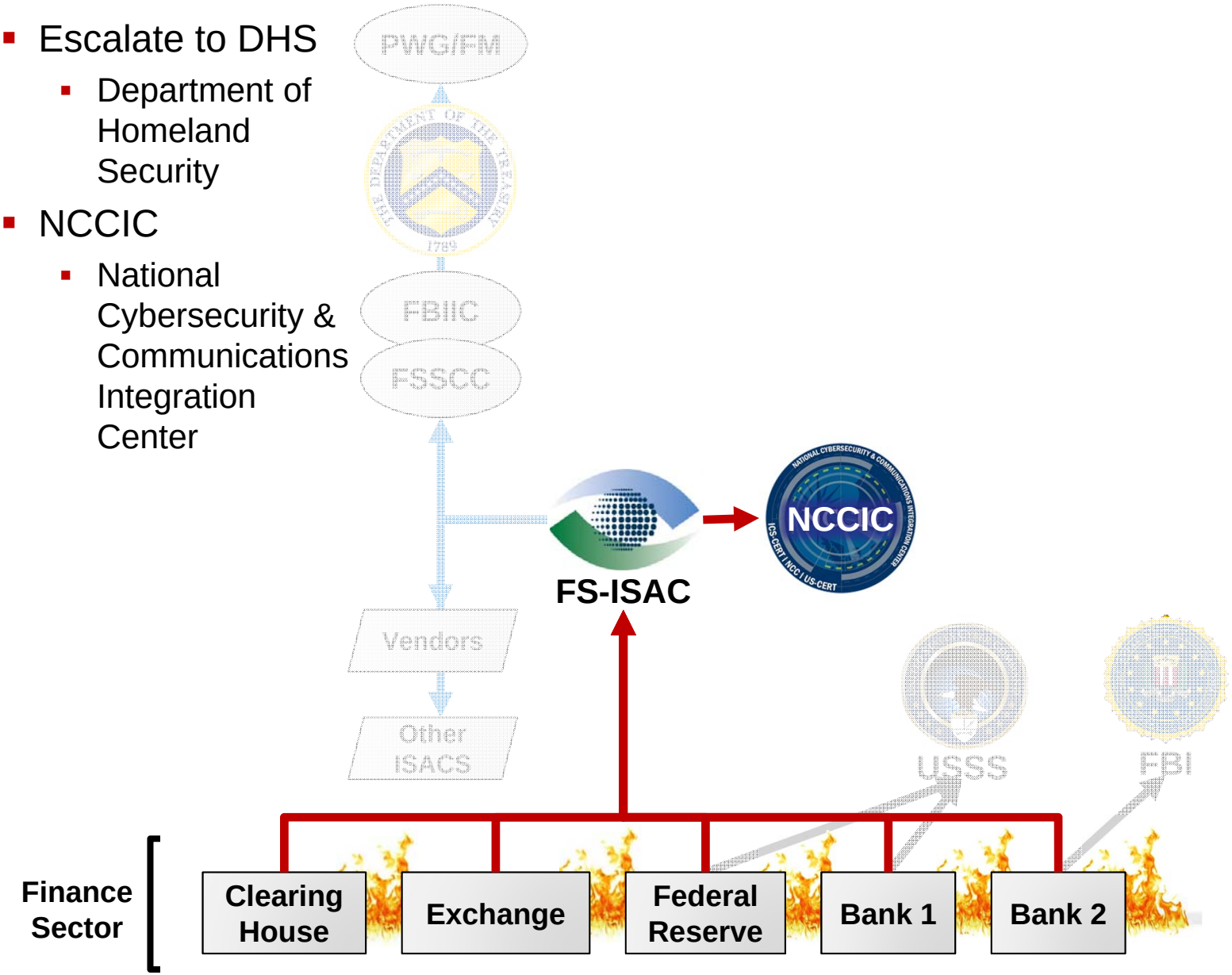
If markets are melting…



- **Treasury**
  - Escalate to senior leadership, *especially* political appointees…
- **President's Working Group on Financial Markets**
- The highest level of financial decision-making
  - Handled no differently than any other financial crisis
  - Secretary of the Treasury, SEC, CFTC, Chairs of the Federal Reserve Board,

On the *cyber* response side

- Escalate to DHS
  - Department of Homeland Security
- NCCIC
  - National Cybersecurity & Communications Integration Center



- DOD
- DHS
- CIA
- FBI
- NSA
- USSS
- Justice
- Treasury
- ISACs
- Dept of State
- State
- Local
- Others

NCCIC

- 24x7 Ops Floor
- US-CERT
- ICS-CERT
- NCC for Telco

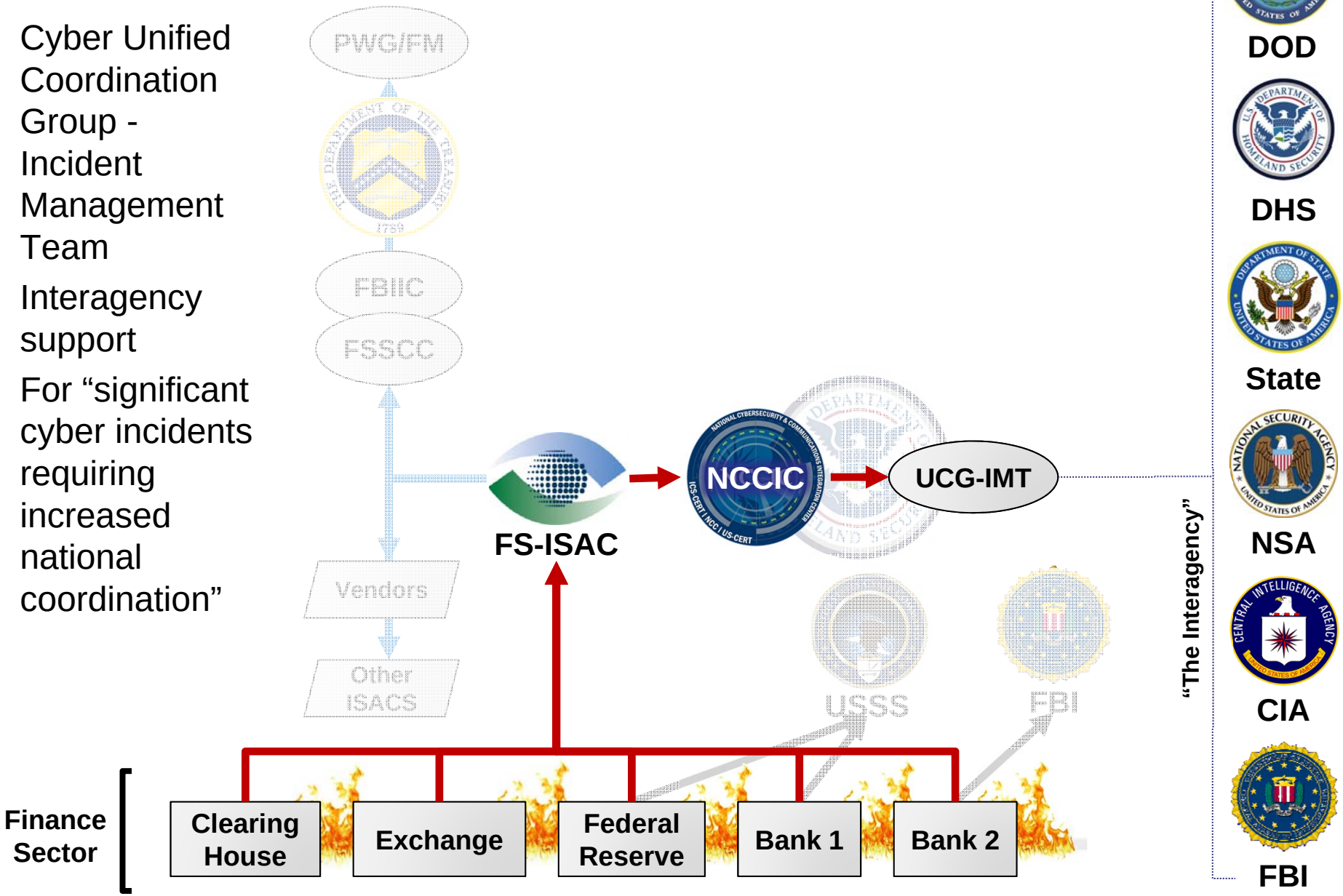
Functions

- Operations
- Planning
- Analysis
- Watch & Warning
- Assist & Assess
- Liaison

BOSTON UNIVERSITY

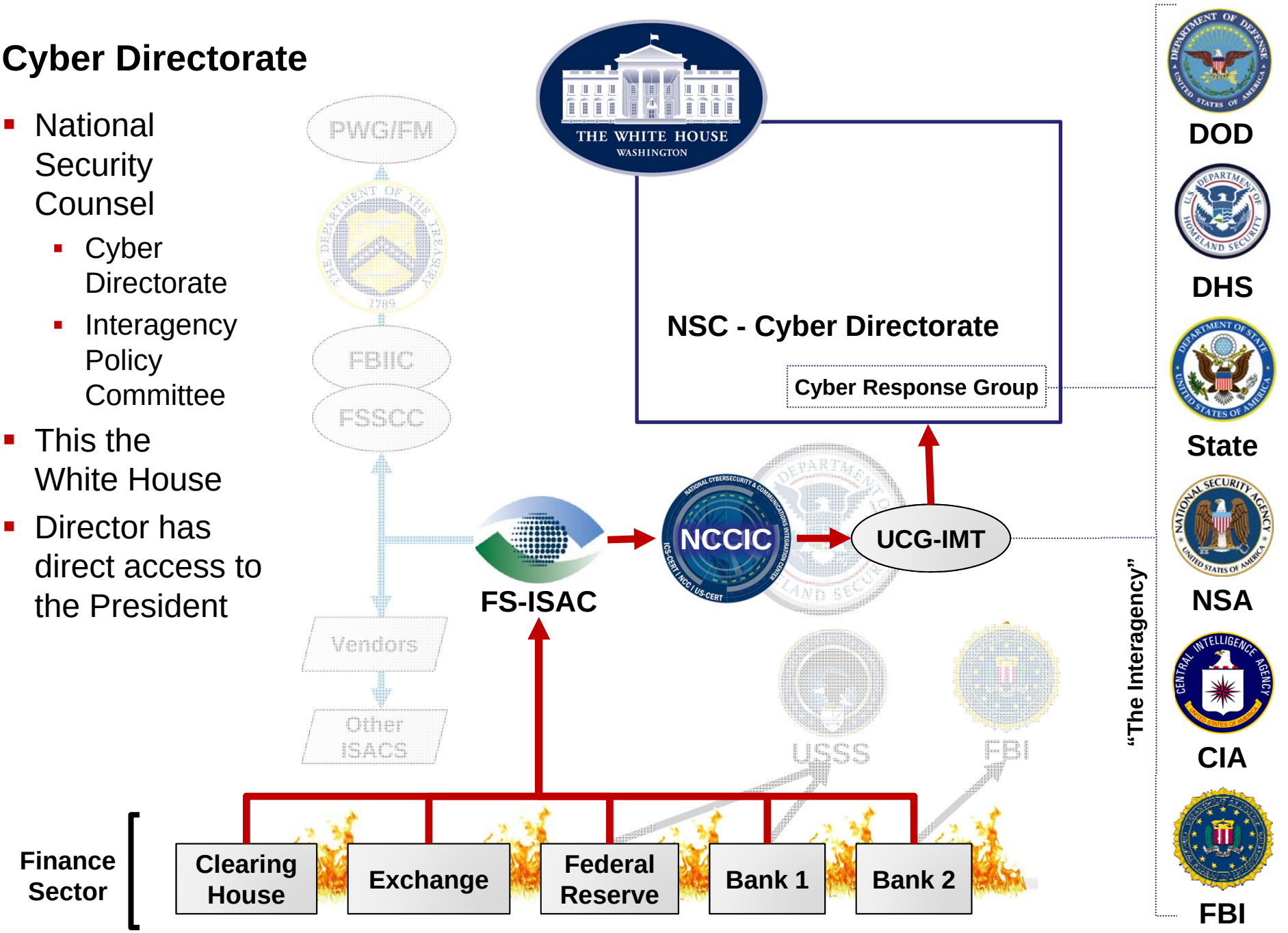
UCG-IMT

- Cyber Unified Coordination Group - Incident Management Team
- Interagency support
- For “significant cyber incidents requiring increased national coordination”



Cyber Directorate

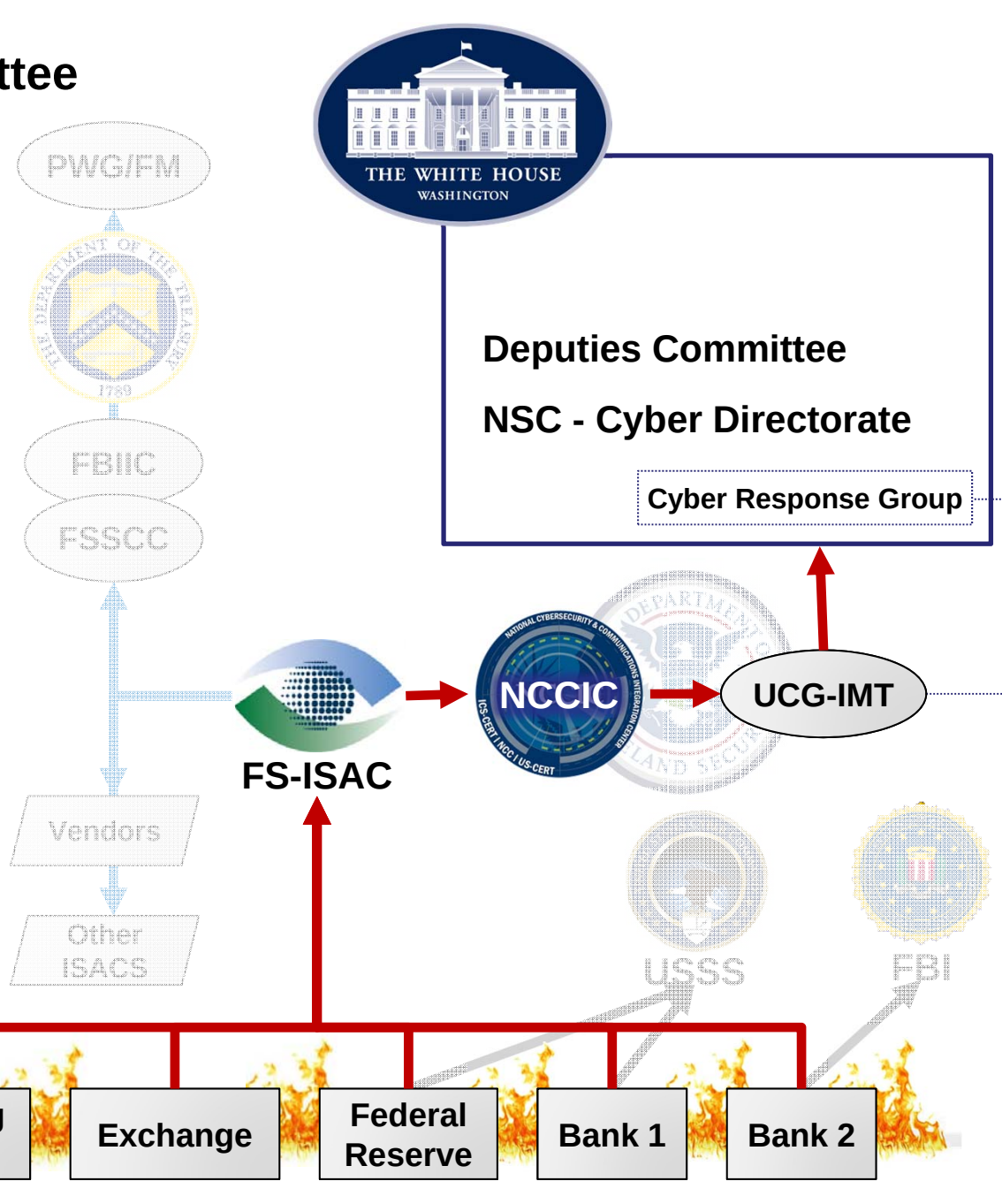
- National Security Counsel
  - Cyber Directorate
  - Interagency Policy Committee
- This the White House
- Director has direct access to the President



Deputies Committee

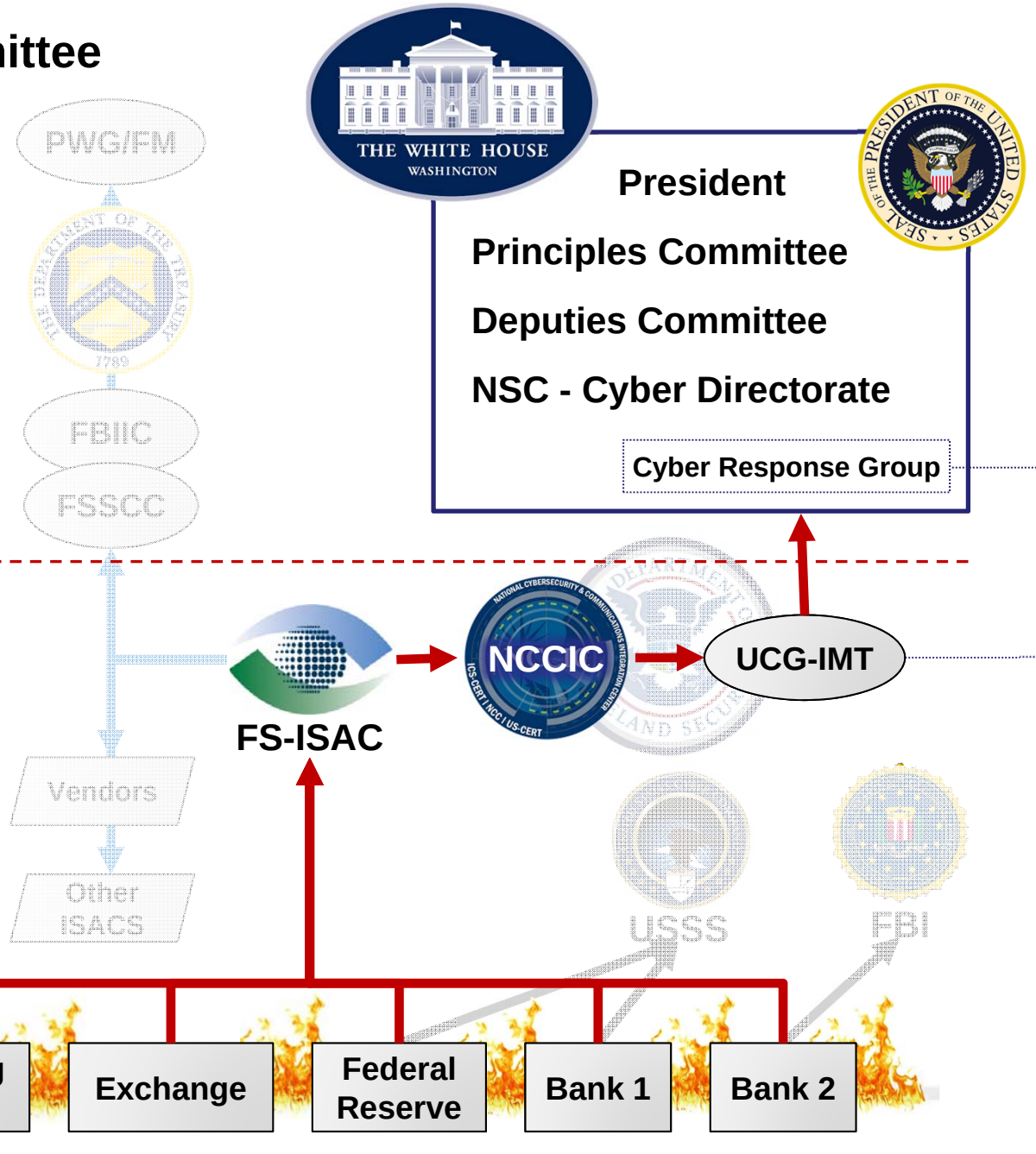
- Deputy Secretary of Defense
- DS of Homeland Security
- DS of Justice
- etc…
- + Experts

- Here you have a true national emergency



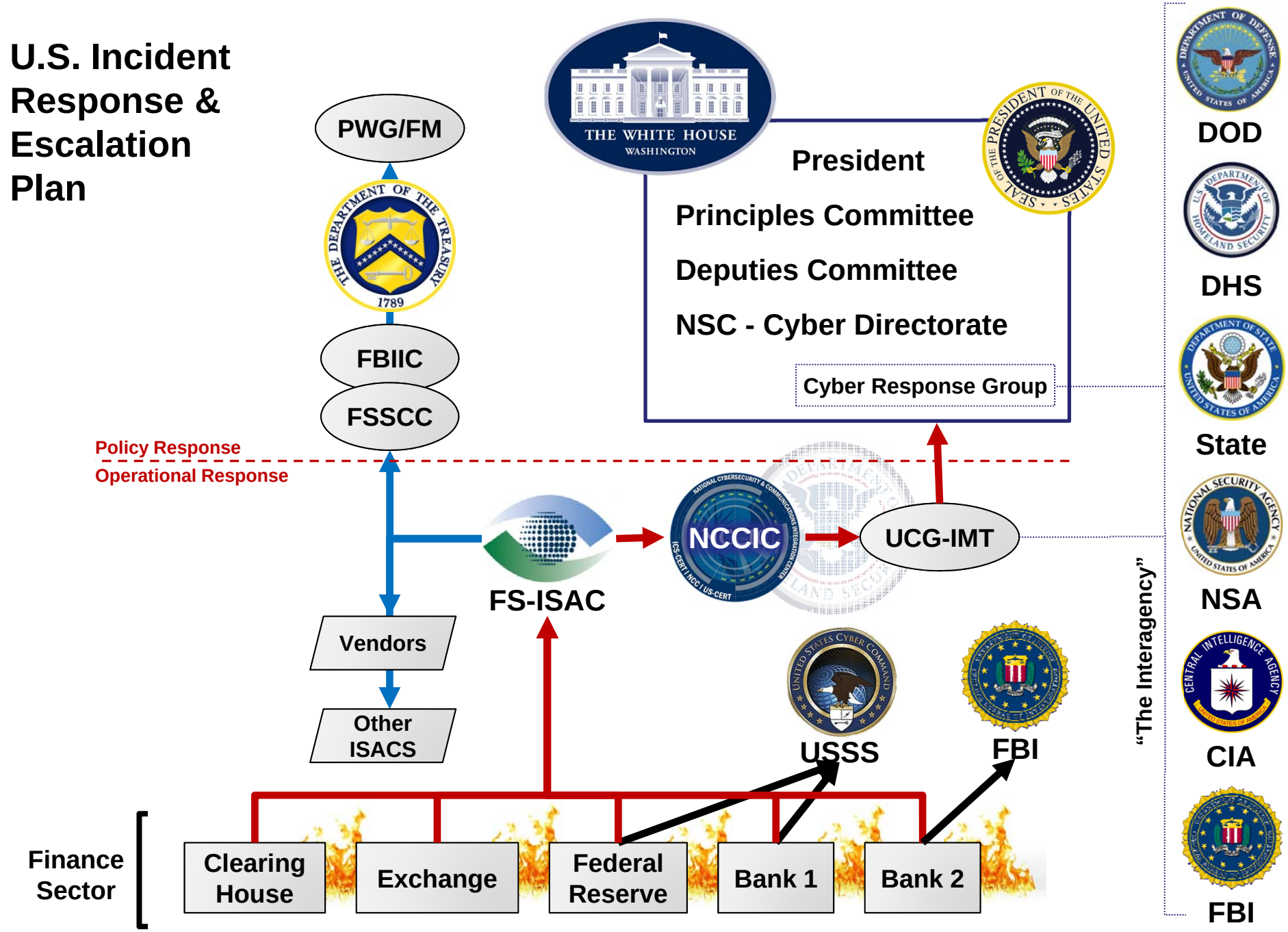
Principles Committee

- President
- Secretary of Defense
- Secretary of Homeland Security
- etc…



- Transition from technical/ops to Policy

U.S. Incident Response & Escalation Plan



Advantages

- As the situation escalates, the process changes from cyber crisis decision makers to And national crisis decision makers
- It leverages time-tested National Security crisis management processes

- Enables national level technical response options
- Places the decisions with those with the power to create additional resources
  - Money, personnel, intelligence
- Enables response using the levers of National Power
  - Diplomatic, economic and military (if it comes to that)

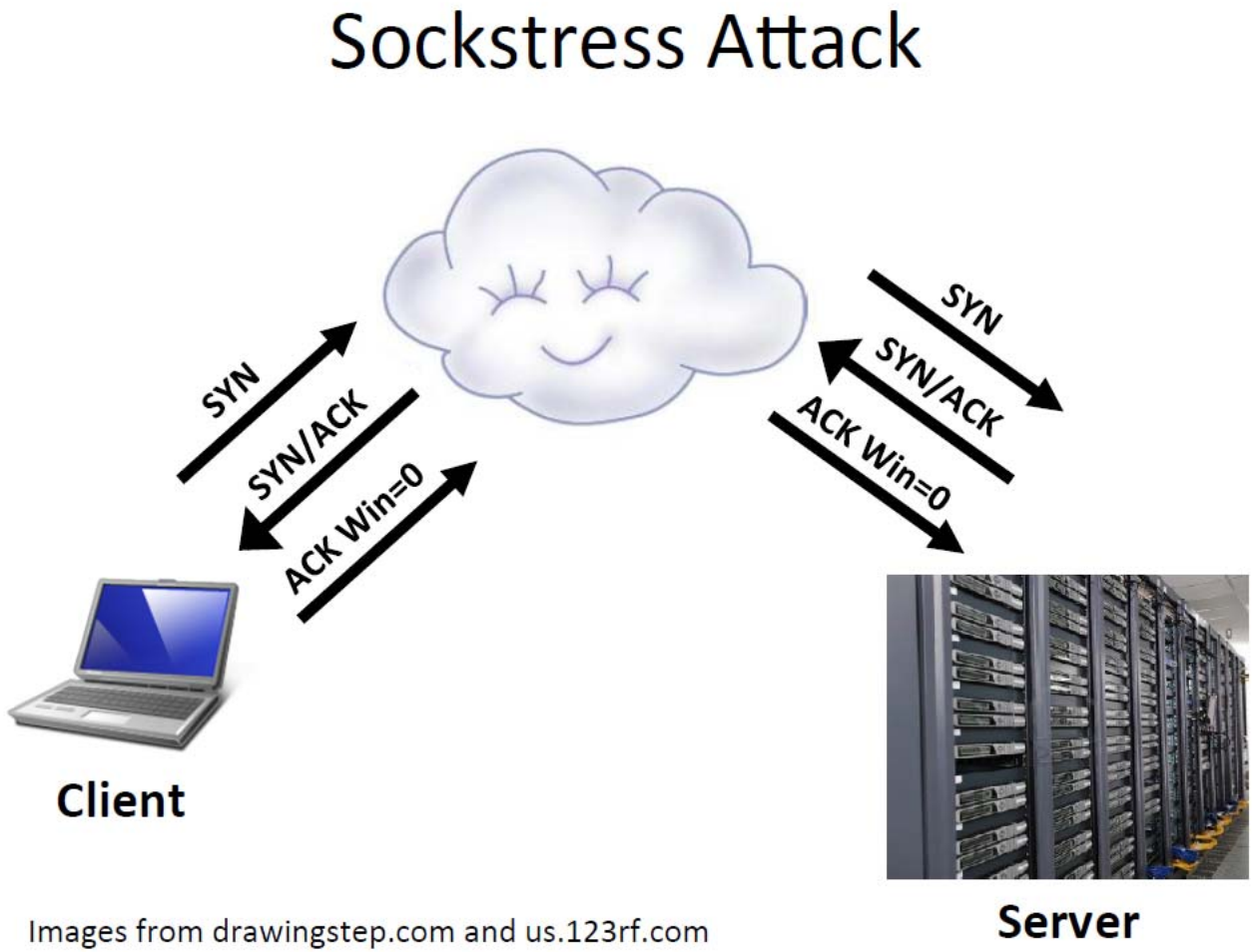
Sockstress DDoS

Killing boxes dead

BOSTON UNIVERSITY

Attack

- Sockstress
  - Establish a handshake
  - Set window size to 0
  - Send that back as your ACK

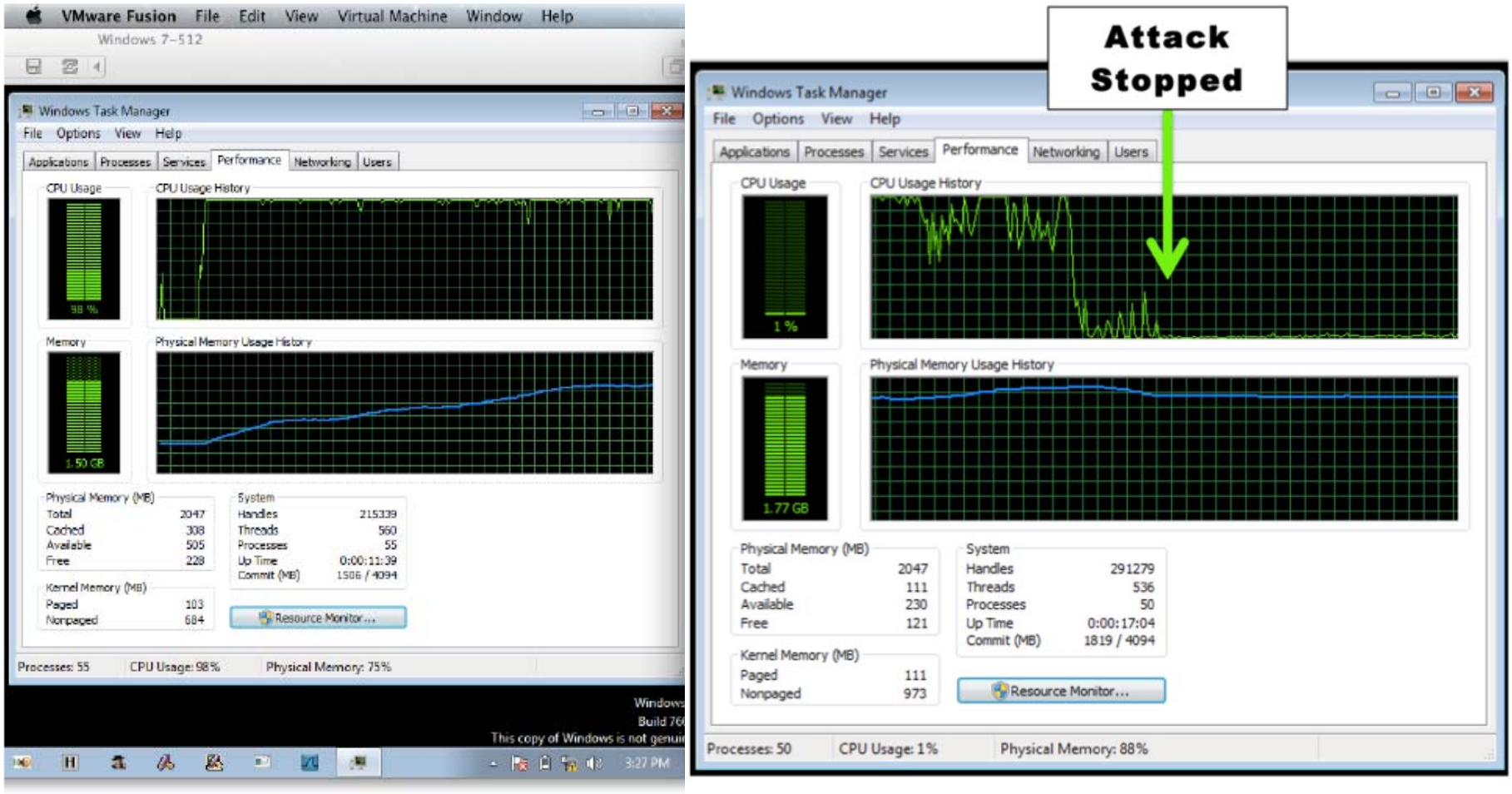


Images from drawingstep.com and us.123rf.com

Application

- This is a layer 4 attack. It will work over the internet
- From inside a network, can simulate a botnet worth of addresses with a single box
- Use an ARP poisoning script to tell anyone who asks that any IP address is me. Attacks then come from 126 IP addresses to a dozen or so ports (Slackware)
- Almost everything with a TCP/IP stack is vulnerable to this at the moment

Sockstress Impact



Mitigation

- Now: Set firewalls to block packets with small window sizes
- Long term: Vendors need to supply an OS patch to reclaim ram
  - This attack was created five years ago but has not been used popularly since, because the person that created it died before he could spread the word...
  - With the Power and effectiveness of the SpamHaus DDoS, it will be way more popular soon

The SpamHaus DDoS was easy

BOSTON UNIVERSITY

“Breaking the Internet”

- Talk: Evil DOS Attacks and Strong Defenses [Scott Bowne and Matthew Prince]
- The SpamHaus attack push 300 GB of sustained traffic a second
- It did not actually “break the Internet”, But it did break DDoS records …and could easily have been much worse
- It was executed by one person using one laptop and five servers, that’s it.

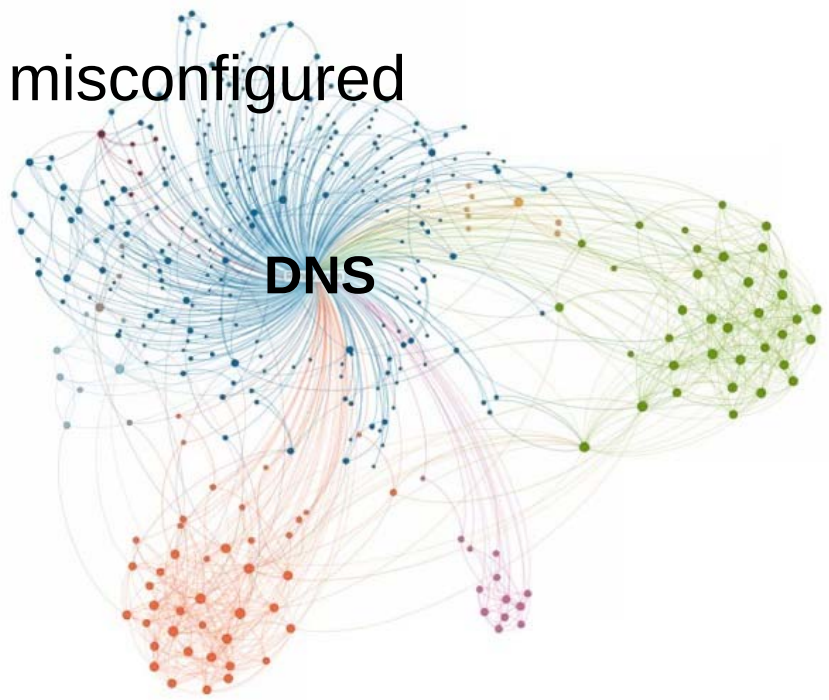
Ingredients

- You don’t need…
  - …a bot net
  - …to coordinate large groups of anonymous people
  - …a ton of technical skill
- You need…
  - …a list of open DNS resolvers
  - …a few servers on networks that allow for IP address spoofing
    - And you don’t need many…

BOSTON UNIVERSITY

Open DNS resolvers

- Not “OpenDNS” the company
- Misconfigured DNS resolvers
  - Pretty much every Android phone with wifi share points turned on…
  - Home wifi points with Bind misconfigured
  - DNS servers. Those that respond to anyone and anything that sent to them



BOSTON UNIVERSITY

One command

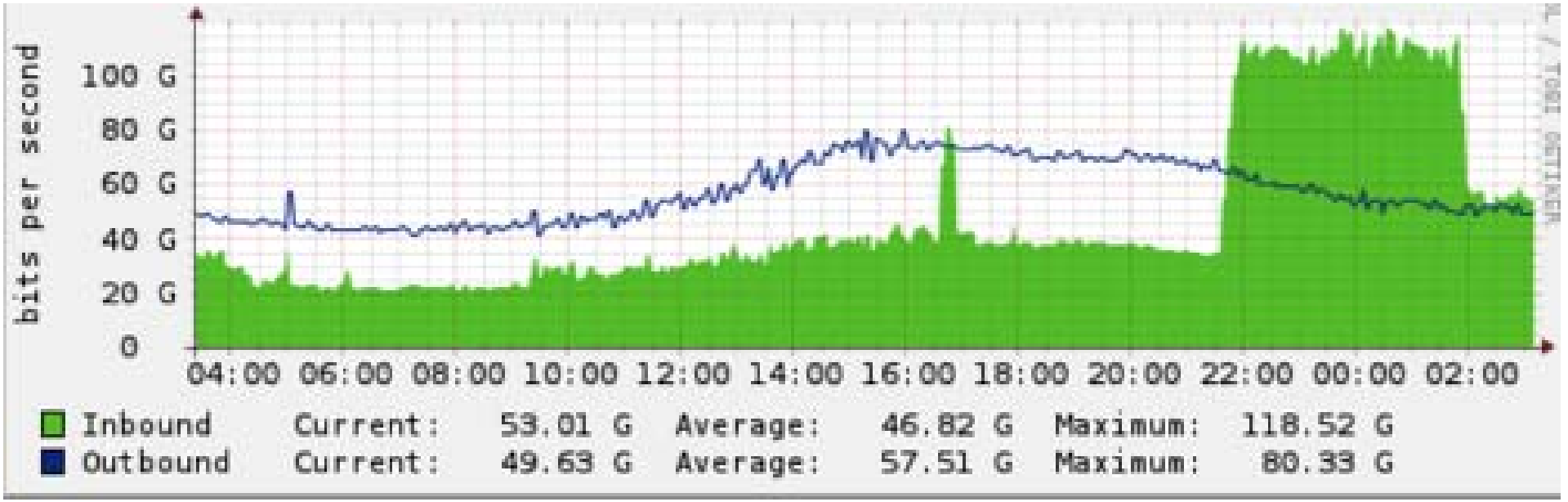
- DNS query (nslookup)
  - -set all (Query to return all the resources available)
  - -t ANY (Any DNS record there)
  - -edns=0 (Give me all the of contents: dnssec, etc…)
  - -notcp (Send up everything over UDP)
  - -buffer=4096 (The largest you can set for UDP packet)
- Amplification
  - 64 byte query
  - 3363 byte response
  - 50x amplification factor

Amplifying the amplification

- To attack others you need one more thing:
  A network that allows source IP address spoofing
- Good routers drop packets “originating” from networks that are not their own [BCP38].
  - Such packets are damaged or spoofed.
- UDP has no handshake,
  - The source can be easily spoofed in the nslookup command
- Like the old Smurf attack (ICMP)

BOSTON UNIVERSITY

A normal DDoS attack



The SpamHaus DDoS attack

The SpamHaus attack

- “The DDoS and that almost broke the Internet”
- 309 Gbps for 28 minutes
- 30,956 open DNS resolvers
- 3 networks that allowed spoofing
- 5-7 compromised servers
- Sent 9Gbps of requests to 0.1% of the open resolvers = 300Gbps attack
- All done by 1 guy with 1 laptop

BOSTON UNIVERSITY

This guy

- (Not really. This was a friend of his.
  The one that talked *on the record* to the NY Times…)

Solving the problem

- Can’t solve the problem from an open resolver standpoint
  - Anyone can install Bind (likely misconfigured)
  - 2013-03-24: 22761875
  - 2013-08-11: 28348485
  - Check yourself @ http://openresolverproject.org/

- Well, you can’t solve it legally…

Imagine the possibilities

- Sent 9Gbps of requests to 0.1% of the open resolvers = 300Gbps attack
- 0.2% 600 Gbps
- 1% 3 Tbps
- 8% 12 Tbps
- The entire U.S. Internet backbone is 24 TB
- The core choke point routers of the Internet are directly addressable

Solution from the other direction

- BCP38
  - "Best current practice" guidance released *13 years ago* (2000) by the IETF (Internet Engineering Task Force)
  - Block spoofed queries
  - Every router (the devices that connect the internet) understands which addresses should be coming from which direction. If a packet arrives from inside the network but the packet claims that it is coming from an IP address outside the network, that packet should be dropped.
- Easy. And yet…
- Almost 25% of networks are *not* set up according to BCP 38
- We need vendors to enforce BCP38 or at minimum make this be the default and force people to turn it off if they *really* need to… (!?)

MDM solutions under attack

BOSTON UNIVERSITY

Mobile Device Management solutions

- Talk: Practical attacks against mobile device management solutions [Brodie]
- Features
  - Set security policies on systems
  - Create a “secure container” In which to run a business applications
    - Encrypt business data
    - Encrypt communications
    - Detect jailbreak/rooting of devices

Mythbusting

- A secure container is only as secure as the underlying OS
  - Just as with regular computers
- There's a huge, highly incentivized community working every day to break into mobile phones
  - Jailbreak detection mechanisms are limited
  - There are no techniques to detect privilege escalation
- "Current [secure container] solutions are useless"

BOSTON UNIVERSITY

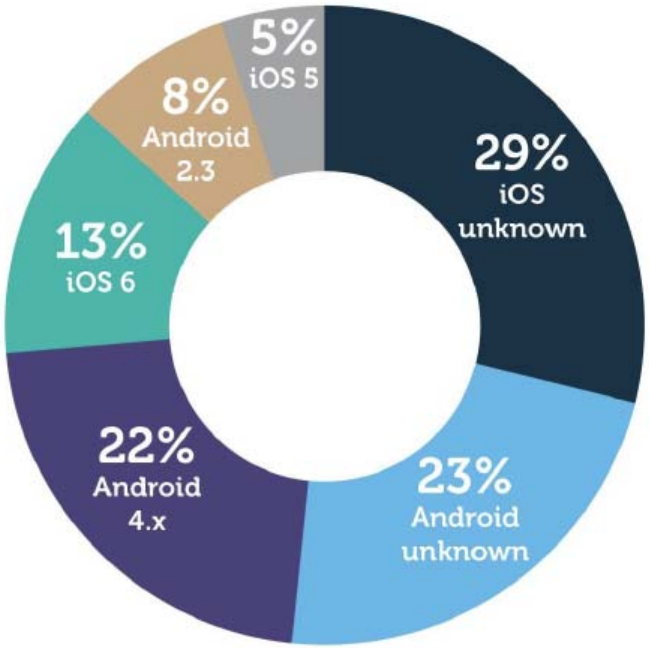
Active attack

- The authors of this talk released concepts and proof of concept code to root and own phones with MDM secure containers.
  - Both Android and iPhone
- Their attack waits until the user reads the supposedly secured message. When it is decrypted into the UI so that the user can read it, their code just goes and picks it up…
  - This was tried using the five most popular sandbox technologies

Survey: Cellular Network 2M Subscribers

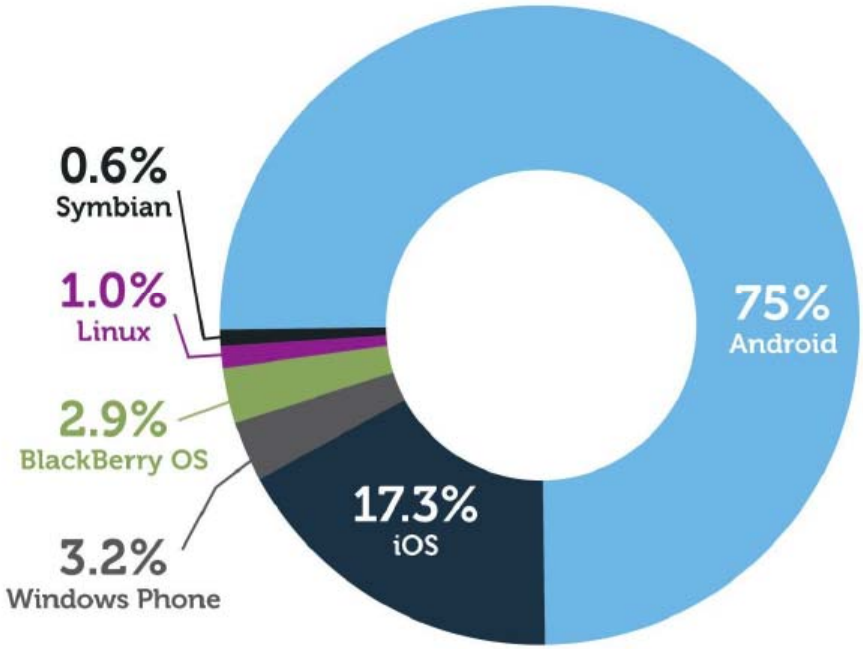
Sampling: 500K

Spyphone Distribution by OS



Count

Mobile OS Market Share



Market Share

Source: IDC Worldwide Quarterly Mobile Phone Tracker, May 2013

LACOON MOBILE SECURITY

What is MDM still good for?

- Management
- Compliance enforcement (preventing user actions)
- DLP
- Physical loss
- Portal – (VM, citrix)

- *Not* protecting your data from malware

BOSTON UNIVERSITY

Creepy DOL

BOSTON UNIVERSITY

CreepyDOL Cheap Distributed Stalking

- Talk: Stalking a City for Fun and Frivolity [Brendan O'Connor – www.maliceafterthought.com]
- How much data can be extracted through passive monitoring of wireless signals
  - Legal (technically)
- Large-scale sensor network without centralized communication
- Cheap

BOSTON UNIVERSITY

Cheap

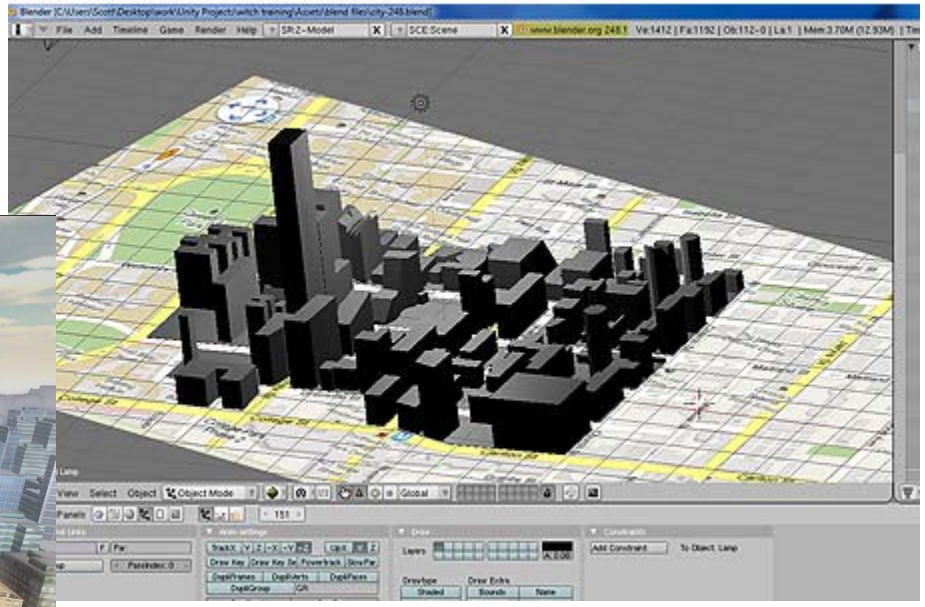
- For less than $60.00 you can build a sensor that can be used to track people's movements throughout your city
  - Raspberry Pi, model A: $8.25
  - Case: $4.61
  - USB hub: $5.00 99 cents
  - Wifi: (2x) $6.52
  - SD card: $6.99
  - USB Power: $1.45
  - Total: 57.08 per node

Open Source

- Radical: Leaderless command and control
  - “Contagion network”
  - Tor + client side SSL + CouchDB + Nginx
  - Grenade-style encryption – pull Pin
- Visualization: Unity game engine
  - Runs on an iPad or Xbox360

BOSTON UNIVERSITY

Results



(I unfortunately have no real screenshots of his real product)

Other Cool Stuff

BOSTON UNIVERSITY

Too many topics to go in to…

- Pwning the Pwnplug
- Hacking a Prius
- Hacking driverless vehicles
- A charger to hack your iPhone
- Making a spy phone
  - TONS of talks on mobile phone hacking
- Owning Networked Home Security Systems
- MITM IPv6
- Hacking Implantable Medical Devices
- A file designed to own forensic software

BOSTON UNIVERSITY

The Status Is Not Quo

- Quinn R. Shamblin
  - qrs@bu.edu

BOSTON UNIVERSITY