NCFTA & CIRFU

Cyber Fusion Center
Pittsburgh, PA

Executive Briefing

Making it Personal.

Brief Chronology…

- **Initiated @ 1997 from PG HTTF & recognized need to included CERT/CC & Other key SME's (Govt Space won't work)**
- **Thoroughly researched via DOJ, FBI-OGC and outside law firms…(data sharing, ownership, IP issues, attribution, augmentation etc…) Can FBI/L.E play? What role?**
- **Need for Jointly owned –Non-Profit entity**
- **Non-Profit Established – registered as 501 © corp in Pa in 2002**

Historical Gaps/Obstacles

- **Lack of “Trusted” Two-Way information sharing relationships with SME’s**
- **Compelled information sharing vs Voluntary - triggers legal issues,**
- **Lack of Neutral setting to analyze/triage open source or Industry owned intelligence (Meet in the middle space)**

Cyber Initiative & Resource Fusion Unit

- Establishes Neutral Space where SMEs can collaborate with L.E. on Focused Initiatives
- Enables 2-way exchange of information between L.E & Industry SMEs
- Leverages exponential resources from key Industry Stake Holders
- Proactively develops referrals and assists Field Level Task Forces as nee

NCFTA/CIRFU Supporting Cast:

Early Developers:

- CERT/CC -CMU
- Rand Corp
- KPMG
- Microsoft
- IBM
- Mellon Bank
- Marconi
- UPITT – WVU
- CISCO
- K&L LLP
- More…

*Separate from Govt/L.E

Recent Partners:

- US CERT/DHS
- Earthlink
- Target Corp
- BSA
- Auction Escrow Co's
- Multiple Financial Srvc
- ISP's – Search Engine Co's
- PSI Inc
- MRC
- Pharma Co's
- AV Co's….
- More…

Focus on Underlying Causes

What is the Threat –Today?

Who is involved – Where?

How do they do it?

What all do they do?

It is Time to

FOCUS ON THE BROADER CRIMINAL NETWORK

EXPANDED FOCUS

What is the best outcome?

Impact = Neutralize.

Recover

Mitigate (IP, $)

Repeat

what works – ID Gaps

Re-Tool

defense/detection

Retrain

staff- Customer

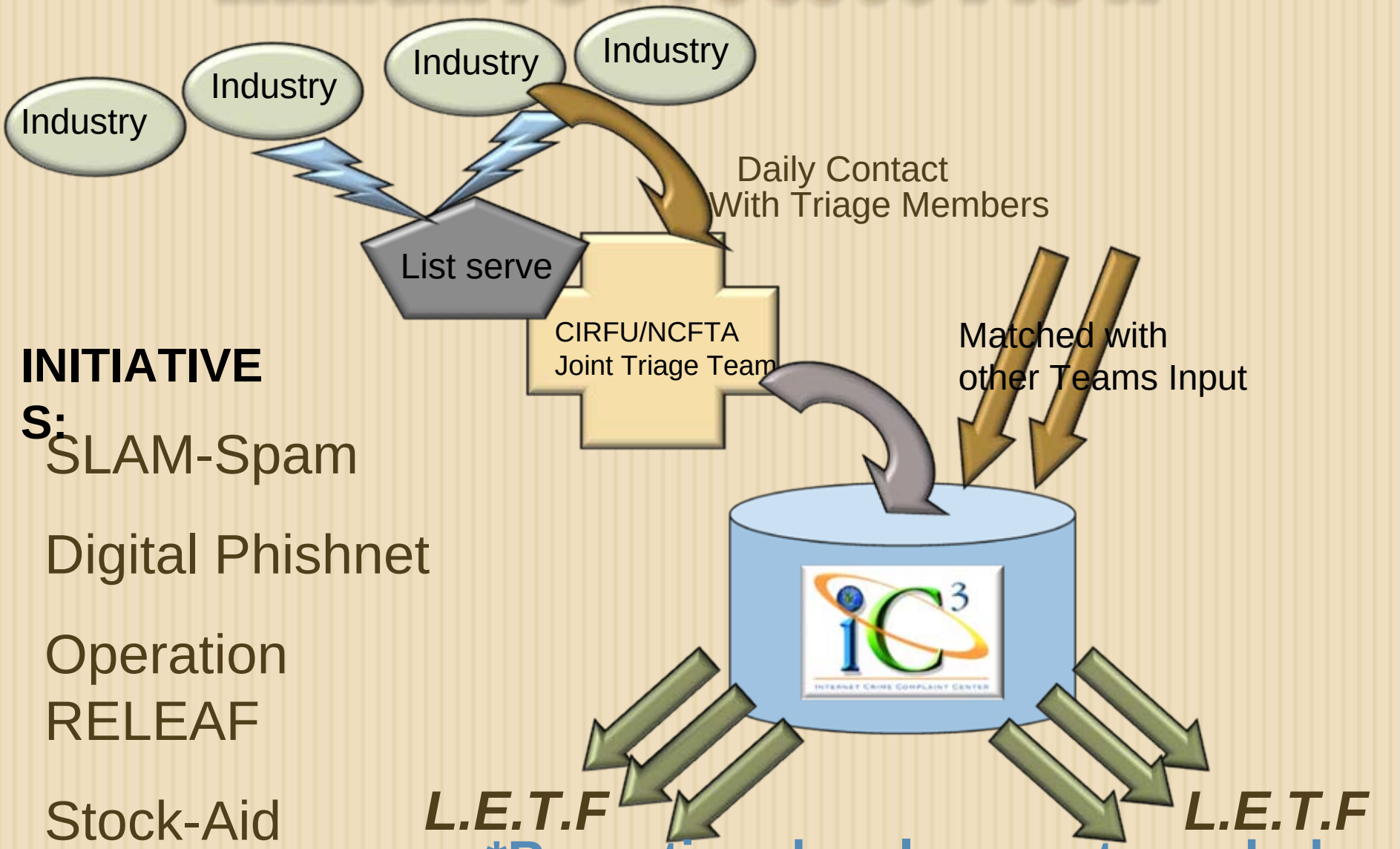
Simulation Lab – (How'd they do that?)

Initiative Based Partnerships

Defining [illegible]m/Threat

Through Industry Perspective

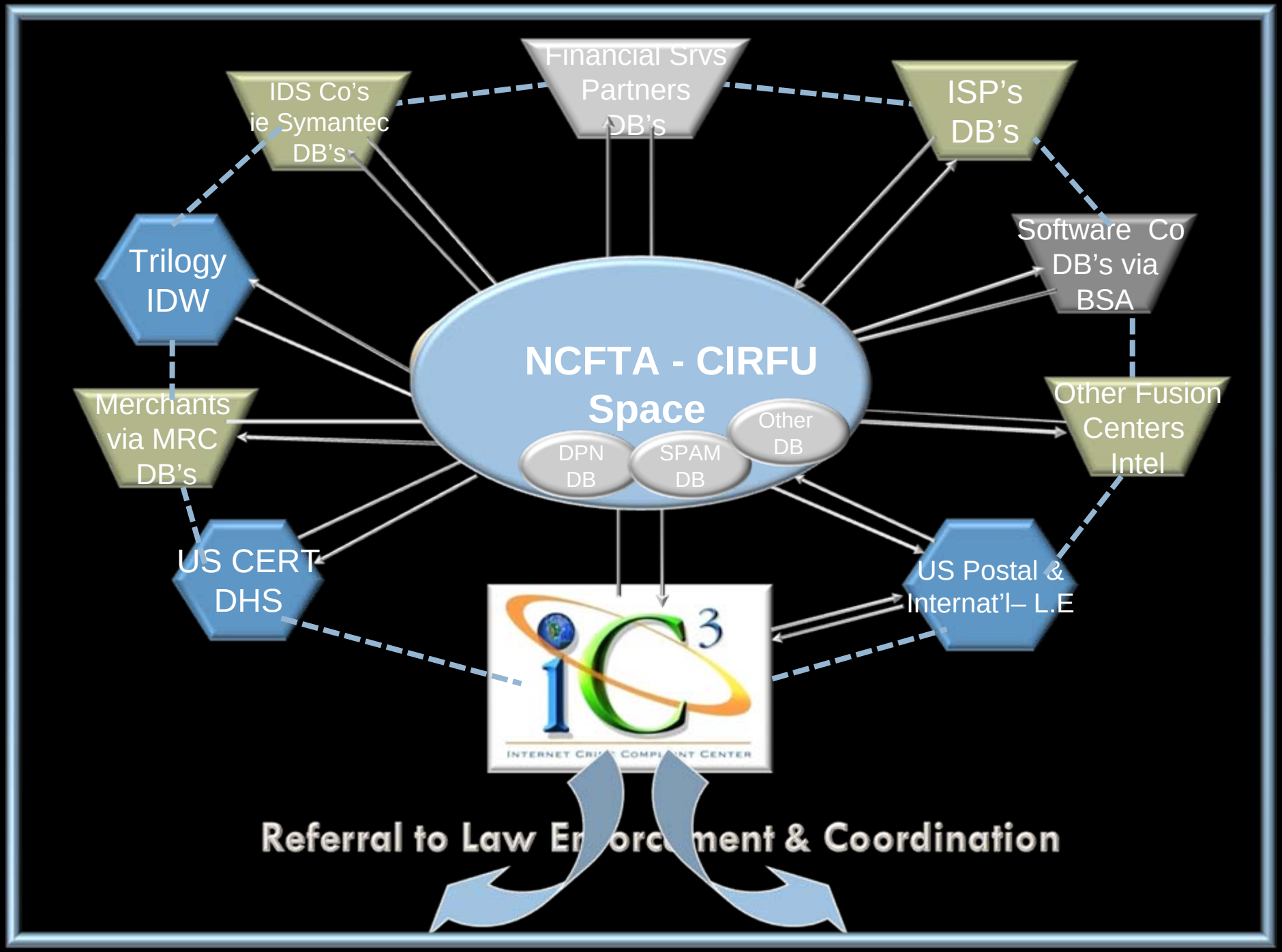
Initiative Process Flow



INITIATIVES:

- SLAM-Spam
- Digital Phishnet
- Operation RELEAF
- Stock-Aid

***Proactive development needed..**


IDS Co's
ie Symantec
DB's
Financial Srvs
Partners
DB's
ISP's
DB's
Trilogy
IDW
Software Co
DB's via
BSA
NCFTA - CIRFU
Space
DPN
DB
SPAM
DB
Other
DB
Merchants
via MRC
DB's
Other Fusion
Centers
Intel
US CERT
DHS
US Postal &
Internat'l– L.E
Referral to Law Enforcement & Coordination

New Success Metrics

- 3000+ ‘harvest’ (‘drop’) e-mail accounts identified associated with phish
  - 150 being preserved this week
- Each ‘harvest’ account contains dozens to thousands of cards/Credentials
  - Average ‘value’ to each card is $5,000 according to several US Court Districts
  - Realistic loss = $300 to $2,000 per card

New Success Metrics

- Total ‘realistic’ very conservative economic loss prevented
  - 3000 accounts * 100 cards/account * $600/card = $180,000,000 USD

*3,000,000+ User Credentials exp..

Overall Benefits

Exponenti l Intelligence…

Enhanced Analytical Ab ity via SMEs

Rapid Case/ ntel Deve opment C pability

Enhanced Cyber Forensics Ability –
including raining Development & Delivery

Human Capita Development – ANALYSTS & AGENTS

Open sources can provide up to 90% of the information needed to meet most U.S. intelligence needs

"Open source is the world of the future."

Eisler, Peter. "Today's Spies Find Secrets in Plain Sight." USA Today 1 Apr. 2008, sec.