Human Capital Development Program





Need/Gap

The need exists for a sustainable workforce comprised of analysts and investigators that can quickly adapt research and intelligence development in line with the continually changing landscape of global cyber crime threats. This will thereby ensure that the needs of industry and Government/Law enforcement towards mitigating/neutralizing these threats are met.

Current Gap acknowledgements

- Training/education for such a work force does not fit into traditional classroom or published curriculum models, as the global threat landscape and resulting needs of Industry and Government/law enforcement are constantly changing, i.e. by the time you publish, the training becomes obsolete.

- The greater majority of meaningful/timely intelligence regarding this evolving threat continues to be owned either by private industry or within the Open-Source environment.

- The needed work force must constantly strive to reinvent itself through a steady stream o f intern/analysts working alongside embedded law enforcement and private industry investigators, those whose job it is to regularly re-evaluate both the threat and the best mitigation/neutralization strategy options.

The NCFTA Model

The NCFTA is the only public/private alliance that has been developed with the above acknowledgements/gaps in mind. Over the past 10+ years, the NCFTA has demonstrated that a model which maximizes the use of a true "collaborative environment" (placing Subject Matter Experts (SMEs) from Industry alongside Government/law enforcement), not only can work, but has proven to be an extremely efficient and effective "best practice" for maximizing resources, expertise, and intelligence development capabilities.

Significant Efficiencies (Time & Money) via the NCFTA Model

- Current efforts to hire/train such a workforce have proven to be extremely costly and inefficient, both within the Government/law enforcement and the private sector. Within the federal law enforcement community alone, more than $300K per FTE is budgeted/spent in recruiting and processing/vetting each prospective employee, before a single person ever reports for work. Further exacerbating this is the recognition that the process itself takes anywhere from nine to twelve months to complete, a timeframe which many prospective employees are unable to endure.
- In contrast, via the NCFTA model, prospective employees are vetted through established industry, law enforcement, and academia relationships and are put through a "hands on" training/orientation process while embedded at the NCFTA facility alongside Government/law Enforcement and industry investigators/ analysts. After a limited background investigation is conducted by Federal Law Enforcement partners, NCFTA interns and analysts immediately begin working on valuable intelligence development projects relative to today's evolving cyber based threats. Because the greater majority of intelligence collected and processed through the NCFTA is either open source or industry owned data, new interns and analysts can begin providing productive support almost immediately.

  Cost/Benefit:
  - $300K & 9-12 months and no return on the investment vs. $3 -5K and two weeks with almost immediate return on the nominal investment, via the NCFTA

  Proven Track Record:
  - Over the past twenty years, the NCFTA has trained more than 150 employees through this means. Of this group, numerous personnel have been recruited/hired by Federal law enforcement and Intelligence Community agencies, as well as a variety of government contractor agencies. (NCFTA Can provide some additional detail here for personnel placed with these organizations- which include FBI, USSS, DHS, USPOSTAL, CIA, Other Intel entities).
  - Through this same time frame, NCFTA Interns/analysts have continue to be hired by many US Financial Institutions (often as their embedded staff) or by Retailers, Pharmaceutical companies, Telecommunications and other partners from various sectors.

Noteworthy Acknowledgements by GAO and Current Administrations

GAO:

In a 2007 report on Cyber Crime the U.S. Government Accountability Office (GAO) acknowledged the economic impacts of these crimes and the resultant threats to U.S. national security. Mitigation efforts noted by GAO included the creation of cybercrime "partnerships" between public and private sector entities designed to facilitate cooperation and information sharing. The GAO specifically acknowledged the NCFTA as this type of partnership example.

Obama Administration:

The NCFTA was recently noted in the President's 60-day, comprehensive, "clean-slate" review to assess U.S. policies and structures for cyber-security. The President's review considered a number of effective public-private partnerships and cited the NCFTA as one of three international examples as an "effective model" which "has a clearly defined institutional mission, well-defined roles and responsibilities for participants, and a clear value proposition that creates incentives for members to participate" and "mitigates concerns that would otherwise discourage participation by establishing and maintaining an environment of trust among the members."[2] In addition, the President's report also suggested the creation of neutral non-profit models (which the NCFTA is) for enhanced information sharing and for developing standards for information sharing. Numerous ongoing NCFTA initiatives have been developed and revised over the past seven years that exemplify these standards.

Participating Entities:

- Guiding structure/content and participation:
    - NCFTA Project Mgr and 1-2 Team Leads (Admin to assist with logistics)
    - US Government/L.E
        - FBI (Cyber, CID and Intel Divisions and HR)
        - USSS (HQ -Investigations and Pitt Field Office)
        - US Postal (HQ and Pittsburgh region)
        - DHS -HSI and CBP (as available)
        - Admin & Grant administration:
            - DOJ – BJA & OJP
            - OPM – with GAO coordination/input
            - Private Sector Options

- Private Sector Partners (Reps from PAC)
    - IAFCI
    - Merchants Risk Council, NRF, RILA
    - FS-ISAC
    - Other key ISACs, REN, MS-ISAC
    - AFP (Other certifying organizations)
- Academia
    - Proven benefactors:
        - UPITT -GSPIA (others), CMU, Mercyhurst, UAB-Birmingham, WVU, Robert Morris, LaRoche, Duquesne, IUP, Colgate, Texas A &M, Georgia Tech, St Vincent, Penn State, Allegheny, George Mason, Marshall, Indiana Univ and others.
        - Ren-ISAC
    - New Academic Partners - TBD

Proposed Funding- going forward: In light of what has already been experienced (based on above metrics) It is expected that supplemental funding would come from:

- Federal Govt/L.E partners
- Private Sector funding partners
- US Grants via DOJ (BJA-OJP)
- Other grant awardees (research and placing Human resources)



Launching the NCFTA Academy – Immersion Program (Draft)

Summary/Overview: (this approach uses "What Works" via the FBI's National Academy and Training)

As the NCFTA model has developed over the past 13 years, (we have further defined the gap this specific model is designed to fill) Re-emphasizing the need for this unique "training" environment – breaking the mold of how L.E and industry can/should work together, and how the changing threat landscape demands a very much "nimble" on-the-fly developing strategy to identify, and then re-identify the most significant threats- and adjust our joint strategy accordingly.

Index of Ongoing Projects/Initiatives at the NCFTA:

NCFTA Projects/Initiatives	**L.E. Projects/Initiatives**
Phishing/ID Theft	BOTNET/MALWARE
Social Engineering/Networks	Forum TFC/Initiative
Forums – Credential harvesting	Financial TFC
Stock-Aid/CyFin/DPN	Romanian TFC
Retail/Reshipping	Russian OC
Pharmaceutical Fraud	IPR and Int. OC
Other IPR & Human trafficking Other – Telco-Mobile	ICAC TBP – Ongoing

Meeting the "Making it Personal" team:

- Introduction to the overall program including primary objectives and Project Managers for each area of emphasis. These will include: 1)NCFTA program leads, 2) Academia Liaison Leads 3) Law Enforcement sponsors and 4) Industry Sector Reps.

Summary follow up and outline of proposed NCFTA -Academy Projects:

- Prepare PR package to Core Industry reps (RILA, IAFCI, MRC, FSISAC, Infragard)
    - Include overall program outline
    - Projected length/scope
    - Projected costs $
    - Optimum expected outcome

- Prepare 1 day executive level overview session addressing the above listed items, with a summary of the course/proposed curriculum, immersion areas, and practical problem exercises.

Proposed Schedule:

Week 1:

- Orientation to all ongoing projects/initiatives
- Resources defined:
    - Available tools - COTS & NCFTA Customized
    - Available SMEs
        - Locally - onsite Industry, academia and L.E.
        - Remotely connected Industry & L.E.
- Metrics redefined And what to expect
    - Expanded view of value likely to be realized through this project.

Weeks 2 -8:

Segment 1	Segment 2	Segment 3	Segment 4
101-201 Immersion	101-201 Immersion	Deeper Immersion	Refined focus on areas most significant to sponsoring entity
Topic A	Topic D	Areas based on critical gaps existing with L.E. & Industry, as well as candidate strengths	Feedback & Evaluation period
Topic B	Topic E		
Topic C	Topic F		

Candidates contribution to projects/initiatives evaluated

** First segment will also be used to evaluate each candidate's skills/capabilities – which may be enlisted to assist with ongoing training/mentoring of other candidates during segments 3 & 4.

Length of time for each segment – estimated to require 2-3 weeks each.

Expectations for participants:

- Guide of Interview/career prospects (Govt & Private Sector)
- Guide/training regarding Resume' preparation and interviewing
- Opportunity for advancement as NCFTA Intern/analyst