Written Testimony for the House Committee on Financial Services Task Force to Investigate Terrorism Financing

Effective Public-Private Partnerships: Lessons Learned from the National Cyber Forensics & Training Alliance

A Statement by Daniel Larkin

Retired FBI Unit Chief and Founder of the National Cyber Forensics & Training Alliance

September 9, 2015

Testimony of Daniel Larkin
Retired FBI Unit Chief and Founder of the National Cyber Forensics & Training Alliance
Written Testimony for the House Committee on Financial Services
Task Force to Investigate Terrorism Financing
September 9, 2015

I. Introduction

Good morning Chairman Fitzpatrick, Ranking Member Lynch and members of the Task Force to Investigate Terrorism Financing (Task Force). I appear today as a former Unit Chief of the Federal Bureau of Investigation (FBI) and founder of the National Cyber Forensics & Training Alliance. I thank you for the opportunity to share with the Task Force some personal experiences I had over the course of my 24+ years with the FBI in developing models for better collaboration between public and private sector subject matter experts (SMEs) to identify and defend against evolving cyber-based threats. I understand that the Task Force is also interested in functional models that might be used to better enable private sector organizations to collaborate with government agencies, including law enforcement, in the fight against international money laundering and terrorist financing. I believe the National Cyber Forensics & Training Alliance (NCFTA) is such a model.

In order to understand how the NCFTA model was developed, it is helpful to consider the following:

- How we define cyber threats is important, and that definition needs to evolve as the nature of globally spawned cyber threats evolves.
- Historically, law enforcement tended to organize its efforts into silos, leading to a narrow view of threats and leaving many cases unaddressed.
- The majority of significant criminal cyber-based threats involve organized crime and money laundering.
- The vast majority of computer networks belong to the private sector.

- As a result, most of the early warning signs – i.e., most intelligence on the threat – reside with the private sector and the private sector is most often best suited to identify those anomalies.
- This private sector intelligence, although sensitive in nature, is most often not classified.
- With cyber, law enforcement needs private industry help more than vice-versa.
- Trust is critical to public/private collaboration, both between the government and the private sector and with the public at large, and it needs to be earned.
- Public/private partnerships must be structured to protect privacy and promote transparency. Personal information, the content of communications, and other private material must not be shared with the government absent lawful process. All sharing must be lawful. In addition, the arrangements for, and the type of information shared, should be transparent to those involved and the public. Private sector working in neutral space – not within government space – can contribute to that effort.
- Public/private collaboration within Government space can inhibit the ability of private sector partners to access and share their real-time intelligence, significantly hindering collaboration.

II. An Early Foundation – Computer Emergency Response Team Coordination Center (CERT/CC)

In 1994, I was re-assigned from FBI Headquarters to the Pittsburgh Division of the FBI. No Federal law enforcement agency in Pittsburgh was large enough to essentially "go it alone". As such task forces were more the norm than the exception. The spirit of cooperation was, and still is, strong there.

As members of this Task Force may know, the first Computer Emergency Response Team Coordination Center (CERT/CC) was established in the 1980s at Carnegie Mellon University in Pittsburgh, and was initially funded by the Defense Advanced Research Projects Agency (DARPA) of the Department of Defense. The developing relationship between law enforcement and the CERT/CC was instrumental to the formation of the NCFTA.

In 1997, it became evident that more and more business was moving to the Internet and, not surprisingly, so were the criminals. At the time, FBI Pittsburgh participated in numerous

task forces addressing a variety of criminal activity. In meeting with Financial Crimes Task Force members, FBI raised the idea of evolving at least part of our Task Force to a Cyber-High Tech Task Force. I initially gained support for the idea from other key Federal agencies as well as State and Local law enforcement. I then suggested that we include the CERT/CC representatives, as they had become experts relative to cyber-related threats and were essentially right in our backyard.

III. Addressing Private Sector Concerns of Working with Law Enforcement

Upon approaching managers from CERT/CC to participate in the developing Cyber-High Tech Task Force, I was surprised to learn that members of the CERT/CC were reluctant to work with the FBI (or other Federal law enforcement agencies) because of concerns that:

- The FBI would force organizations to reveal sensitive potential vulnerabilities they had shared on a confidential basis with CERT/CC.
- The FBI would possibly "drag" organizations into a prosecution which also could reveal the organization's potential vulnerabilities to the public.
- The FBI would create disruptions that would impede organizations' ability to conduct business and defend themselves against cyber threats.

I explained that the FBI and other agencies had become more sensitive to private sector concerns, and that the FBI was committed to prove that in order to gain their trust. I suggested that the FBI begin an immersion program, where an FBI Cyber Agent would be detailed to the CERT/CC to serve as "a fly on the wall" and offer support for CERT/CC and their clients, without negatively impacting their relationship.

Within the first six months of this program, the embedded FBI agent was able to help CERT/CC and two of their clients more fully understand the scope of threats they were facing, based on prior knowledge the agent had of similar incidents. Later, CERT/CC staff and their

clients worked cooperatively with the FBI to help identify threat/actors who were ultimately prosecuted, with no negative impact on the relevant company.

CERT/CC management and I later met to propose expanding the immersion program to include more law enforcement and private sector representatives, based on the recognition that the project became successful only because people sat together and collaborated. The setting encouraged individuals to get to know each other and collaborate; the environment helped to develop trust among participants and became an early principle of the NCFTA model. It was also important that the relationship was transparent, and there were appropriate procedures between the two separate spheres (public and private).

IV. Focus Group Meeting Leads to Core NCFTA Model

By this time (1998) Pittsburgh had developed a strong and growing base of high technology and financial services organizations. From this base, approximately 30 cross-sector organizations were invited to a Focus Group meeting to consider embedding resources together in order to better collaborate in the common fight against international cyber threats. Out of this Focus Group, a white paper was developed which summarized the core objectives and potential returns on investment of a new public/private alliance—which eventually became the NCFTA. These objectives included:

- Creation of a neutral "meet in the middle" environment where the government and private sector could collaborate in a timely and efficient manner.
- An organizational model that brings together private sector stakeholders with domestic and international law enforcement representatives to build trust and to identify, mitigate and ultimately neutralize significant global cyber-security threats.
- The creation of joint initiatives based primarily on a consensus view of priority threats from the private sector, with law enforcement support being sought secondarily. The theory being that if industry consensus is large enough, law enforcement will find a way to assist.

- Space should be primarily designated as Sensitive but Unclassified (SBU), with all participants undergoing background investigations tailored to their role and responsibilities.
- Creation of a simulation lab (or malware lab) where various network platforms could be simulated to evaluate how certain malware might behave, appear and be detected and mitigated.
- Participants would be vetted SMEs and be expected to share knowledge and expertise.
- Sharing of threat/risk intelligence would remain confidential with Non-Disclosure Agreements (NDAs) executed between partners to protect proprietary information.
- Joint training would be developed to ensure a common understanding of permissible private sector involvement and information sharing.
- Lawful access to appropriate law enforcement resources would be developed and streamlined.
- Training on best practices would be developed and refined regarding newly identified threats and the proper handling of digital data that might ultimately assist in combatting cyber threats.

V. Official Establishment of NCFTA as a Non-Profit

After considering several organizational options for formally establishing the project, a local law firm offered to research alternative models, taking into account the proposed vision and objectives outlined above. After approximately one month of research, the firm suggested that a 501(c)(3) non-profit entity be established to serve as that neutral "meet in the middle" body. This organizational model allowed public and private entities to establish relationships via different means, such as through representation on a Board of Directors or through a broader Board of Advisors. Over the following 18 months, a group of volunteers from the Focus Group crafted a business plan, articles of incorporation and bylaws to advance the process. Finally, in 2002 the NCFTA was officially incorporated as a non-profit in the state of Pennsylvania.

VI. Proving the Model Works

Over the succeeding 13 years, numerous investigative initiatives were developed through NCFTA with cross sector partners, spawning hundreds of investigations involving hundreds of criminals, both domestic and foreign. A common thread through many of these investigations has been international organized crime, money laundering, and in some cases ties to terrorist financing.

What began as a regionally supported effort also has shifted to an international and, from a Federal law enforcement perspective, headquarters-supported project. All law enforcement embedded at the NCFTA are assigned to their respective Headquarters, enabling them to serve as a better resource for industry in getting cases developed and assigned globally.

The NCFTA, in partnership with the FBI, also has expanded the "make it personal" objective internationally, hosting annual International Task Force sessions for three months each year. Over the years, representatives from numerous countries have spent time as embedded partners at the NCFTA, developing joint investigations and an enhanced rapport with U.S. law enforcement and private sector partners.

Today, numerous private sector organizations embed SME resources at the NCFTA alongside a growing pool of domestic and international law enforcement. Hundreds of additional SMEs connect to the NCFTA via various real-time communication channels set up to facilitate the expanded collaboration. Extensive information regarding the NCFTA and its initiatives is available at www.ncfta.net.

VII. Lessons Learned

So what are some of the lessons learned from the evolution, establishment and operation of NCFTA?

- Significant global threats may initially manifest themselves in a variety of ways known only to the private sector, and their significance may not be understood until the information is pooled.
- Early warning intelligence may give the appearance that the threat is routine or common, such as a common phishing or ID theft scheme. However, with an expanded focus through NCFTA, it may actually turn out that the scheme is part of a much larger campaign with many more tentacles and a potentially more significant impact.
- Cyber criminals will enlist many different and creative schemes to generate funds, such as through coordinated networks of domestic and international money mules, prepaid reloadable cards, virtual currency and other means. Monitoring, detection, mitigation and responses must also continue to evolve with the same creativity.
- Using a private model, in the case of the NCFTA a 501(c)(3) non-profit entity, can make open and transparent public-partnerships easier.
- The NCFTA model leverages "existing" resources by giving them a better environment in which to perform. From this perspective it is a very efficient work force multiplier.
- Relationships are vital to make collaboration work, and they can also be fragile.
- Making it personal--knowing your partners' perspective and needs--is essential to success.
- The human capital development benefits of the NCFTA model are substantial.

VIII. Conclusion

Thank you again for the opportunity to come before the Task Force today and share some of my experiences as an FBI agent and founder of the NCFTA. I would be pleased to answer any questions the Task Force may have regarding my experiences with the establishment and operation of the NCFTA or the benefits of public/private partnerships like NCFTA.