NATIONAL CYBER-FORENSICS AND TRAINING ALLIANCE

Collaborate strengthen brand protection, law enforcement, and Industry alliances

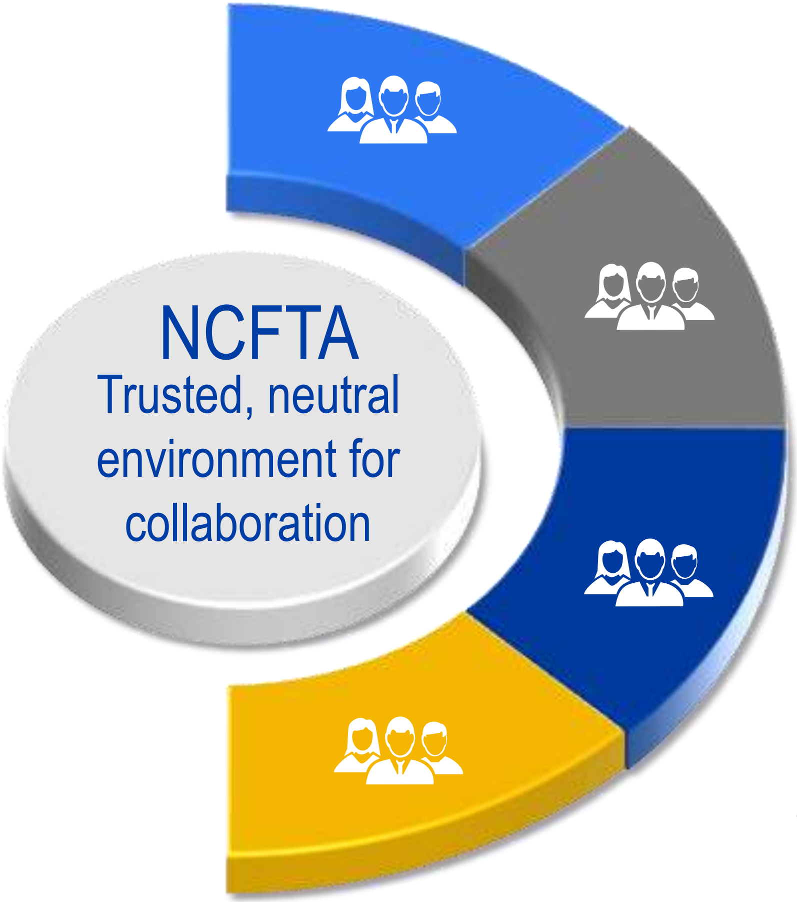
THE NATIONAL CYBER-FORENSICS AND TRAINING ALLIANCE
20
YEARS
NCFTA
EST. 2002
IDENTIFY • VALIDATE • DISRUPT

NCFTA - ORIGINS OF A PUBLIC-PRIVATE PARTNERSHIP MODEL

2002

- Law enforcement and private industry acknowledged a mutual dependency
- *Actionable* two-way information sharing is critical but was not occurring
- Face to face relationships are most effective to establish trust
- A neutral environment was needed to enable fair, trusted, and active sharing
- NCFTA was established as a 501c3 non-profit
- Expansion office located in New York

NCFTA ENVIRONMENT



Private Industry

On-site and virtual community of cross-sector industry committed to working together to identify common risk, share mitigation strategies, and helping law enforcement focus on most impactful issues

NCFTA

Dedicated **team of intelligence analysts**, access to 20+ years of information, committed to operationally supporting industry and law enforcement

Law Enforcement

On-site domestic and international law enforcement partners committed to disrupting cyber crimes and cyber enabled criminal activities and enterprises

SME Community

A trusted community of subject matter experts and **cyber superheroes** committed to making a difference for the greater good

NCFTA OBJECTIVES FOR INFORMATION SHARING

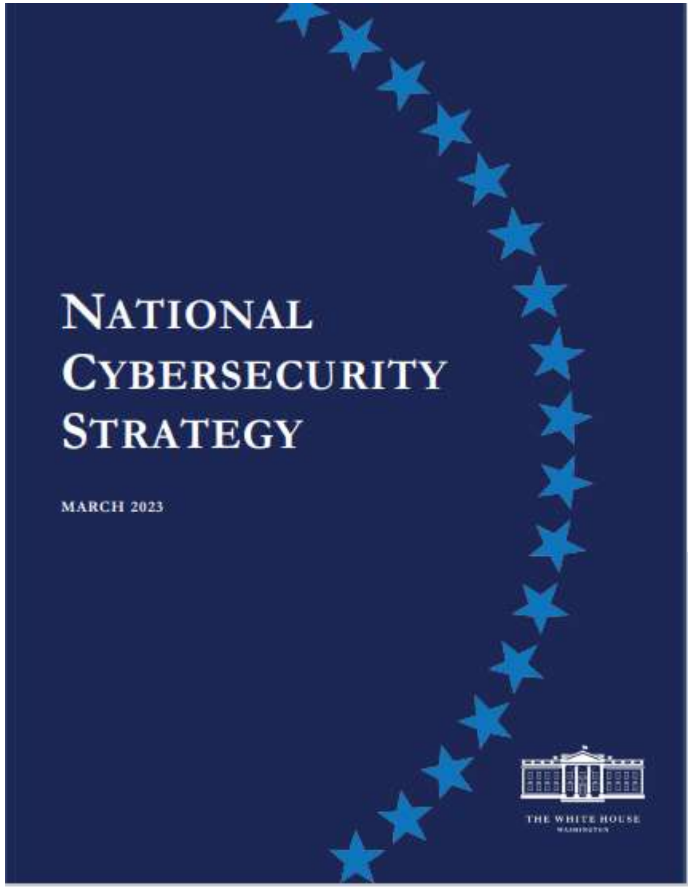
IDENTIFY	Identify risk, threats, and threat actors impacting our cyber ecosystem (via active information sharing)
VALIDATE	Confirm assumptions
MITIGATE	Share mitigation strategies to help make everyone more resilient
DISRUPT	•Leverage law enforcement and judicial process to disrupt those miscreants responsible for the criminal activity: •Disrupt criminal infrastructure •Indictments/Arrests

NCFTA INFORMATION SHARING MODEL

Filling the Gaps

- Gov't agencies can't possibly answer, respond or address every issue
- Share information once
  - With law enforcement, industry peers and across different industry sectors
  - *All participants have control over how information is used
- Make information **actionable**
  - NCFTA enhances data (using internal data, other partner information, research)
  - Industry informs law enforcement about the most impactful issues
  - **Actionable** for industry to protect itself and for law enforcement to disrupt actors

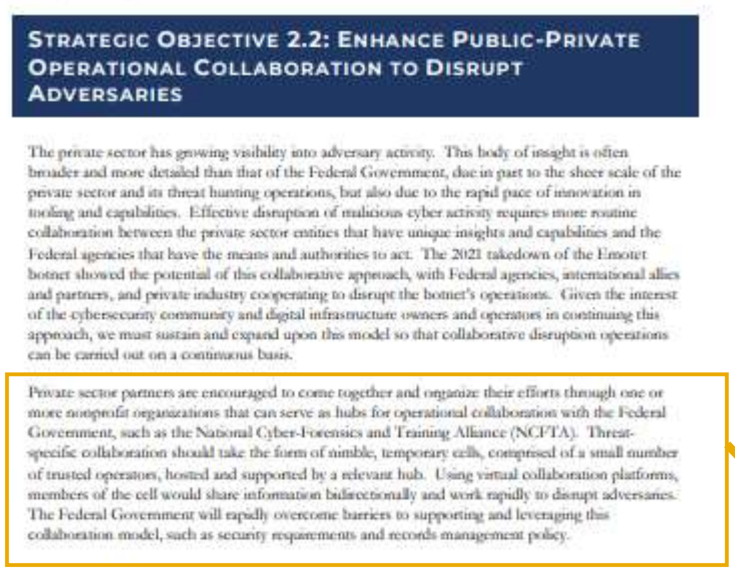
NCFTA RECOGNIZED



NATIONAL CYBERSECURITY STRATEGY

MARCH 2023

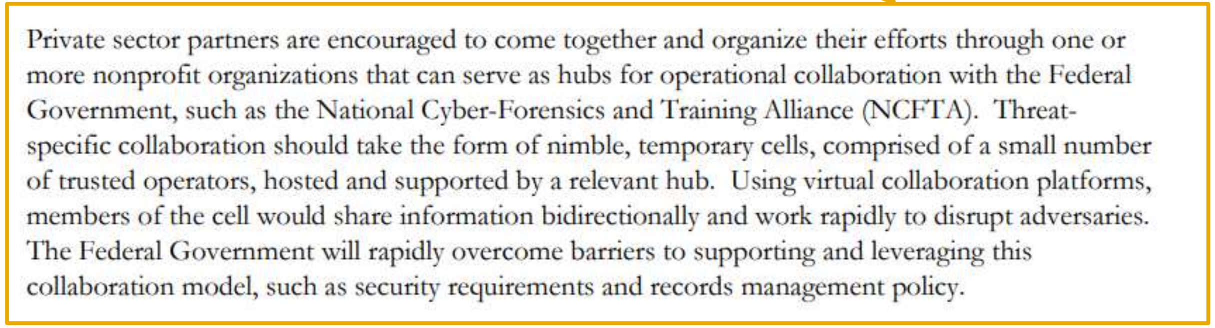
THE WHITE HOUSE
WASHINGTON



STRATEGIC OBJECTIVE 2.2: ENHANCE PUBLIC-PRIVATE OPERATIONAL COLLABORATION TO DISRUPT ADVERSARIES

The private sector has growing visibility into adversary activity. This body of insight is often broader and more detailed than that of the Federal Government, due in part to the sheer scale of the private sector and its threat hunting operations, but also due to the rapid pace of innovation in tooling and capabilities. Effective disruption of malicious cyber activity requires more routine collaboration between the private sector entities that have unique insights and capabilities and the Federal agencies that have the means and authorities to act. The 2021 takedown of the Emotet botnet showed the potential of this collaborative approach, with Federal agencies, international allies and partners, and private industry cooperating to disrupt the botnet's operations. Given the interest of the cybersecurity community and digital infrastructure owners and operators in continuing this approach, we must sustain and expand upon this model so that collaborative disruption operations can be carried out on a continuous basis.

Private sector partners are encouraged to come together and organize their efforts through one or more nonprofit organizations that can serve as hubs for operational collaboration with the Federal Government, such as the National Cyber-Forensics and Training Alliance (NCFTA). Threat-specific collaboration should take the form of nimble, temporary cells, comprised of a small number of trusted operators, hosted and supported by a relevant hub. Using virtual collaboration platforms, members of the cell would share information bidirectionally and work rapidly to disrupt adversaries. The Federal Government will rapidly overcome barriers to supporting and leveraging this collaboration model, such as security requirements and records management policy.



Private sector partners are encouraged to come together and organize their efforts through one or more nonprofit organizations that can serve as hubs for operational collaboration with the Federal Government, such as the National Cyber-Forensics and Training Alliance (NCFTA). Threat-specific collaboration should take the form of nimble, temporary cells, comprised of a small number of trusted operators, hosted and supported by a relevant hub. Using virtual collaboration platforms, members of the cell would share information bidirectionally and work rapidly to disrupt adversaries. The Federal Government will rapidly overcome barriers to supporting and leveraging this collaboration model, such as security requirements and records management policy.

NCFTA Programs and Initiatives

Brand & Consumer Protection

- Intellectual Property (IPR)
  - General Counterfeits
  - Automotive
  - Apparel
  - Consumer Goods
- Illicit Tobacco
- Pharmaceutical Fraud
- Illicit Substances
- E-Commerce Fraud
- Internet Fraud Alert (IFA)

Cyber Financial

- Account Abuse and Intrusion
- Advanced Payments Abuse
- Transient Criminal Groups
- BEC Fraud & Money Mules
- Payment Card Fraud
- Cryptocurrency
- Human Trafficking
- Securities Fraud
- Synthetic Identity

Malware & Cyber Threats

- Malware Analysis and Decryption
- Onsite Malware and Gaming Lab
- Honeypot/IoT Monitoring
- APTs and Other Threat Groups
- Dark Web Analysis
- Threat Actor Attribution and Engagement
- SIEM Support
- Controlled Purchases and Analysis

MULTI-LINGUAL INTEL ANALYSTS — RUSSIAN / CHINESE / SPANISH / ROMANIAN
Custom research & intelligence reports, incident support, law enforcement coordination

TLP AMBER FOR NCFTA PARTNER USE ONLY - NOT FOR PUBLIC DISSEMINATION

The Importance of Joining the Fight Against Counterfeiting

- Counterfeiters affect so many different industries and the health/safety risks that occur in each industry differ

General Counterfeits

Apparel & Footwear

Automotive

Illicit Substances

Pharmaceutical Fraud

Counterfeit Tobacco

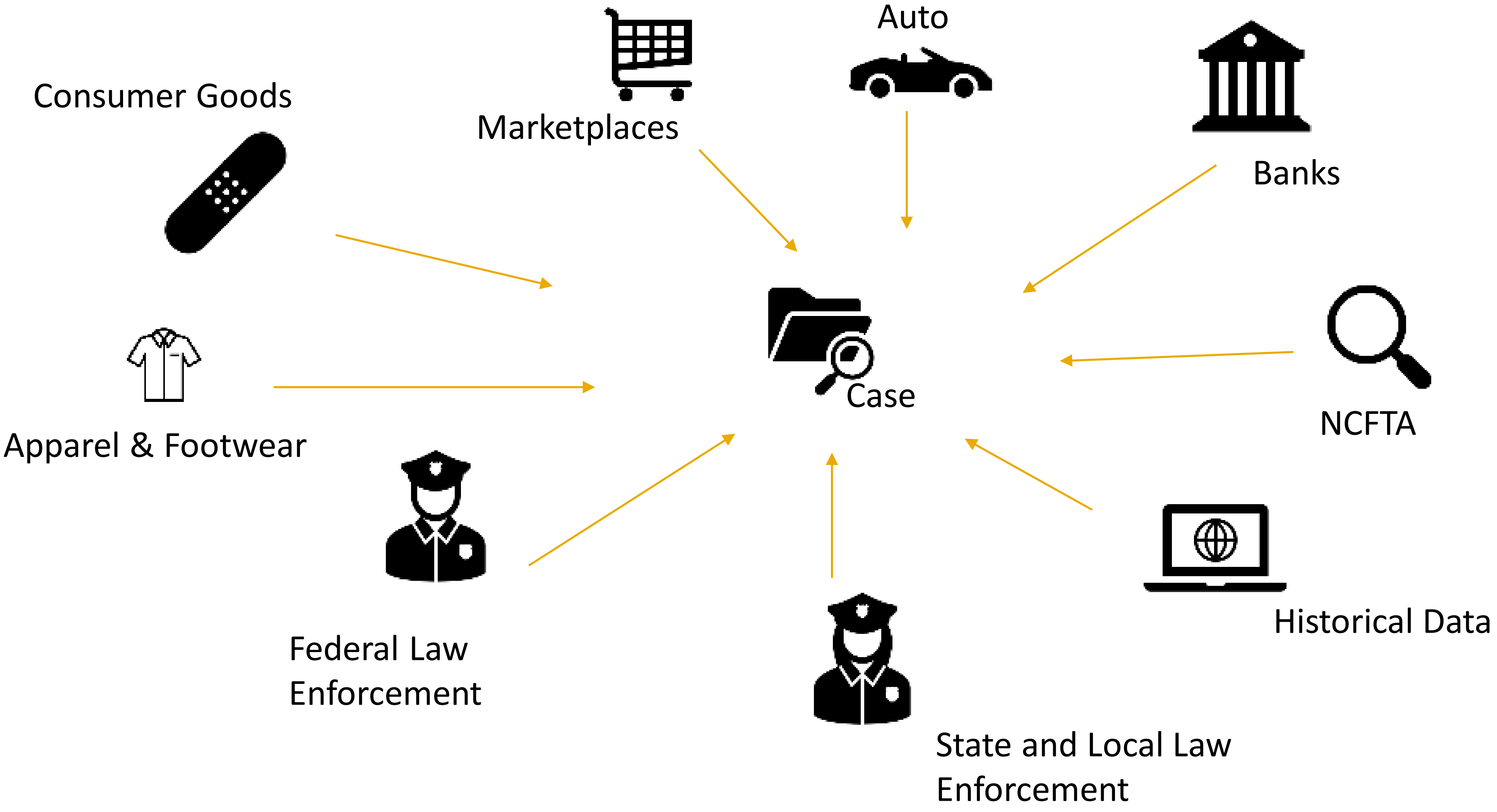
Consumer Goods & Medical Devices

Music Streaming Content

Retail/E-Commerce

Microchips

NCFTA INFORMATION SHARING MODEL



New Trends to Protect Trademarks

- 3 Dimensional Trademarks
- Design Patent Registrations
- Local State Trademark Regulations
- Local State Legislation
- Easter Egg Trademarks

NATIONAL CYBER-FORENSICS AND TRAINING ALLIANCE

Jason Kosofsky
jkosofsky@ncfta.net
810-278-7926