CYBER DIVISION
FEDERAL BUREAU OF INVESTIGATION

Cyber Division Talking Points
OAS Inter-American Committee against Terrorism (CICTE) Talking Points
Friday, February 26, 2016

FBI Cyber Overview:

Mission Statement: Identify, pursue, and defeat cyber adversaries targeting global U.S. interests through collaborative partnerships and our unique combination of national security and law enforcement authorities.

- **Vision Statement:** Global Leaders for Intelligence Led, Threat Focused Cyber Operations
  - [Note: Intelligence led in everything we do, not JUST operations]

- **State of Cyber Division:**
  - Sweeping Changes Since 2012 (Next Gen Cyber)
  - Ensure Effectiveness – Meet the Evolving Threat (Action Oriented)
  - Whole Government Approach to Combating Cyber Threats (Cyber Task Force)
  - National Program Management Approach (Threat Teams)

- **CyD Strategic Vision:**
  - We constructed a 5-year plan that outlines our strategy for maximizing technological tools and capabilities, developing a highly skilled workforce, building and maintaining highly valuable private partnerships, and providing timely and predictive intelligence to drive nationally coordinated and targeted operations.
  - CyD founded in 2002; National Strategy not published until 2006
  - 2006: CyD had four strategic objectives:
    - Intrusions and malicious code
    - Online predators
    - Intellectual property violations
    - Internet fraud
  - 2012: Next Gen Cyber rollout: Computer Intrusions
  - 2013: Development of Five Year Cyber Strategic Plan
    - Drive the direction of the program over the next five years
    - Assist with setting priorities, driving alignment, and simplifying decision making
    - Five "focus areas," which will drive our strategic development:

Outreach and Information Sharing: Achieve an integrated global network of active and trusted partnerships to collectively defeat cyber adversaries

Operations: Lead a unified, multinational team of law enforcement and intelligence agencies in executing global, strategic operations to dismantle the cyber threats facing the U.S. and its allies

Intelligence: Provide real-time, predictive intelligence to support the USIC's ability to prevent or preempt strategic surprise

Workforce Development: Define, develop, acquire, and utilize available resources and partnerships to build the finest cyber investigative entity possible

Technology: Identify and deploy technically sophisticated, cost-effective solutions to enable operations, analysis and collaboration

- **Cyber Task Force:**
  - Each field office has a CTF and CETF
  - CTFs are enhanced with TFOs and OGAs
  - CTF: Investigating intrusions, led in the field by a cyber squad supervisor but have strong centralized program management within CyD. This program management aspect is critical due to the global aspects of cyber attacks.
  - Cyber investigations require close coordination within the Intelligence Community, large private sector companies, and foreign partners.
  - CTFs are composed of all Special Agents/Intelligence Analysts currently working Computer Intrusion Program (CIP) matters, Computer Scientists, Task Force Officers currently working CIP matters, and CNCI Special Agents/Intelligence Analysts.
  - CETF: Identify, investigate, and pursue the successful prosecution of individuals and groups responsible for crimes against children, will be led in the field by a criminal squad supervisor. They are program-managed at FBIHQ by CID.
  - CETFs are composed of Special Agents, Intelligence Analysts, and Task Force Officers currently working Innocent Images and Crimes Against Children matters.

- **STRAT/TAC Initiative**
  Past Challenges

    1. Technical collection spread out instead of centralized – inability to ascertain a holistic overview of the threat.
    2. Too many cases on the same threat actors across multiple field offices.
    3. Critical Example: 288 Legion Jade cases across 47 field offices

4. 2800 Investigative Cases
    4.1. 49% Criminal
    4.2. 41% National Security
    4.3. 10% Attribution is not yet determined
    4.4. 25 Legion Sets

Solution: Cyber Threat Team:

To solve this problem, we have been working to create a model that will effectively address priority cyber **national security** threats by maximizing the benefits of a well-coordinated **threat-centric** model.

1. Our Cyber Threat Teams will consist of:

- **Strategic Threat Execution Office (STRAT)** – Leads in the development and execution of the FBI's mitigation strategy against the specific threat

- **Tactical Threat Execution Office (TAC):** Works specific issues related to a threat in support of the investigative and operational strategy set by the STRAT; Supplies additional resources & continuity of operations

- **CyD Threat Manager (TM):** Establishes the national strategy against all threats in coordination with the USIC and other strategic partners (Five Eyes); maintain comprehensive view of all STRAT/TAC assignments to ensure the proper alignment with prioritized threats

This model will allow us to allocate resources more effectively against the threats, prioritize threats more effectively, optimize scalability, and help us develop a stronger cadre of subject matter experts.

This will not immediately affect the way we investigate criminal cyber threats.

What are the Cyber Threats .....where do we begin:

- We work with three partner groups: industry partners, international partners, and USIC to develop intelligence on the threat.
- The FBI makes a policy of not disclosing the details of any one case of a U.S. victim of malicious computer network operations, be they private citizens or businesses. This includes the recent Chase disclosure.

- We *do* commit ourselves to disclosing technical indicators of known nefarious actors, as well as assessments of imminent and trending threats, gained by way of our extensive network of intelligence sources.
- These disclosures include hard copy reports, and threat briefings offered to private sector, academic, and law enforcement partners at every classification level. Our sharing efforts cover all cyber threats, including threats from credit card and phishing schemes, hacktivists, professional transnational cyber criminal organizations, nation-state actors, and cyber terrorists.

Cyber Threat Actors:

- **Actor Types**:
  - Cyber Terrorists
  - Nation States
  - Hacktivists
  - Financial Motivated Groups/Individuals
  - Insider Threats

- **Cyber Terrorists**
  - A growing threat as our world becomes increasingly wired.
  - April 2013, the AP Twitter account was hacked and a message was sent out stating that there was an explosion at the white house. This caused stock markets to dip in the blink of an eye.
  - Actors are seeking to use cyber means to impact and disrupt our lives.
  - Not very skilled at present, but getting better and learning to use readily available tools.

- **Nation States**
  - Nation States get the most media coverage, especially in light of the recent actions of Edward Snowden.
  - Potential targeting of critical infrastructure via destructive means.
  - Use of Computer Network Exploitation to facilitate access within a network (gathering of network diagrams from network admin machines, escalation of privileges to install malware at the enterprise level).

- **Hacktivists**
  - Looking to advance an ideology or social cause.

- Denial of Service Attacks (DDOS) – According to Verizon's 2014 Data Breach Investigations Report, more powerful Botnets and reflection attacks have helped drive the **scale of DDOS attacks up 115 percent since 2011.**

- **<u>Financially Motivated Group/Individuals</u>**
  - Despite all the media attention given to the actor types I have previously mentioned, **<u>this is the Growing Threat to your company)</u>**.
  - DHS reports, the **average cost of a cyber attack is $9,000**
  - DHS reports, **Cybercrime costs the world significantly more than the global black market in marijuana, cocaine, and heroin combined.**
  - According to CNN Money (article published online, 6/13/14), "Hacked companies have exposed the personal details of 110 million Americans –that's half of the nation's adults."
  - Fraudulent wire transfers
  - ATM/Money Mule scams
    - Skimming – The physical installation of a "skimmer" on an ATM, gas pump, or POS terminal, to read your card data as you pay. [swiping before pumping gas]
    - **Stat: 87 percent of skimming attacks were on ATMs** [Verizon's 2014 Data Breach Investigations Report.]
  - **Retail Point of Sale (POS)**
    - When attackers compromise the computers and servers that run POS applications, with the intention of capturing payment data.
    - Stealing credit card info through use of malware
    - According to Verizon's 2014 Data Breach Investigations Report, 85 percent of POS intrusions took WEEKS to be discovered.
    - One of the newest threat vectors we have seen are retailers, and undoubtedly you have heard about the Target breach.
      - **TARGET- 40 million Credit Card numbers and another 70 Million Customer Records stolen (<u>Open Source</u>)**
    - According to open source reporting, additional data breaches have been reported at **Nieman Marcus, Michaels, and most recently, P.F. Chang's China Bistro.** The restaurant was reported to have lost a batch of customer debit and credit card data

- **<u>The Insider Threat</u>**
    - **Insider:** Any person with authorized access to any United States Government resource to include personnel, facilities, information, equipment, networks or systems.
    - **Insider Threat:** The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.
    - Over the past century, the most damaging U.S. counterintelligence failures were perpetrated by a trusted insider with ulterior motives. In each case, the compromised individual exhibited the identifiable signs of a traitor – but the signs went unreported for years due to the unwillingness or inability of colleagues to accept the possibility of treason.
    - Insiders convicted of espionage have, on average, been active for a number of years before being caught.
    - **Cyber Specific Problem**:
        - Increased network usage by employees and associates increases the pool of insiders with access to large amounts of data.
        - Increased enterprise reliance on cloud computing can make data even harder to guard.
        - The insider threat is magnified when we look at the cyber world. Individuals have access to an unprecedented volume and variety of information at an increased velocity.
        - Today more information can be carried out the door on removable media in a matter of minutes than the sum total of what was given to our enemies in hard copy throughout U.S. history.
        - Consequently, the damage caused by malicious insiders will likely continue to increase unless we have effective insider threat detection programs that can proactively identify and mitigate the threats before they fully mature.
    - **Current Threats**:
        - <u>Accidental Leaks</u>: Accidental leaks often take place when an unorganized employee has increased availability and access to sensitive data.
            - One recent example is the Department of Veterans Affairs' settling a class action lawsuit after millions of personnel's private information was stolen from a laptop at an employee's home.

- Disgruntled Employees: This actor seeks to degrade your organization's capabilities by purposefully providing sensitive information to competitors.
    - For example, **Hanjuan Jin** took a leave of absence from her US employer in 2006. While on leave, Jin worked for a similar company in China. A year later, Jin returned to the United States. Within a week of her return, she bought a one-way ticket back to China, and advised her US employer that she was ready to end her leave. Jin returned to work on February 26, 2007 and for the next two days downloaded hundreds of technical documents. On February 28, 2007, during a routine check at the airport, more than 1,000 electronic and paper documents proprietary to her US employer were found in Jin's luggage. In 2012, Jin was sentenced to four years in prison and fined $20,000.

- Sympathizers/Leakers: These actors tend to use their access to vast amounts of data to knowingly and willingly distribute massive volumes of sensitive information publicly.
    - Perhaps the most famous leaker in U.S. history, Edward Snowden.

- Trained Spies: This is not a new threat, and it is one the FBI has been combating for decades.
    - Perhaps the most notorious of these recent cases is Robert Hanssen, a veteran FBI counterintelligence agent who provided highly classified national security information to Russia and the former Soviet Union. Throughout the course of many years of spying for the Russians, Hanssen covertly transferred national security and counterintelligence information to the KGB and intelligence officers assigned to the Soviet embassy in Washington, D.C. and later to officers assigned in the KGB's successor agency, the SVR, in exchange fro over $600,000 in cash and diamonds. In early 2001, Hanssen was arrested at a park in Vienna, Virginia while performing a "dead drop" placing a package containing highly classified material at a pre-arranged site for pick-up by his Russian handler. A year after his arrest, Hanssen was sentenced to life in prison for his crimes. The FBI significantly overhauled its internal procedures on identifying internal threats as a result of Hanssen's activities, creating an internal penetration unit at FBI Headquarters, in addition to refining the processes by which FBI employees have and maintain access to classified

information.

- **Threat Types**
  - Specific Attack Vector
  - Mobile Banking Vulnerabilities
  - Mobile Malware
  - Botnets

- **Specific Attack Vector**
  - DNS (Domain Name Service) Hijacking. Users type in a website, and there is a malware that redirects them to another site.
    - **Example**: In 2013, traffic to the *NY Times* website was redirected to another website. Spearphishing was the method of compromise leading to the DNS Hijacking. [Does not have to be a complex attack, can be as simple as an email.]

- **Vulnerabilities in Mobile Banking**
  - Mobile banking vulnerabilities may exist on mobile devices that are not patched, or where malware is developed to target the use of that device.
    - **Example: Zeus-in-the-Middle** (*mobile version* of GameOver Zeus – not as prevalent but shows risk)
    - Infection can be from malicious app in any appstore or via spear phishing/physical access
    - Once infected, users of infected mobile devices who utilize that device for mobile banking, expose themselves to risk by entering their personal information.

- **Mobile Malware**
  - Some SMS message interception of two-factor authentication
  - Some mobile malware to send spam to send additional mobile malware
  - According to open source information (FYI – forbes.com) infections on **Android OS devices remain a prime target** for mobile malware.
  - Android malware rose from 238 threats in 2012, to 804 threats in 2013, 97 percent.
  - According to the 2014 Cisco Annual Security Report – 99% of mobile malware in 2013 targeted Android

- According to McAfee's First Quarter, 2013 Threat Report – 14,529 new variants

- **Evolution of Botnets**
  - Botnets continue to become more sophisticated and our techniques must evolve to keep pace. We might take down one Botnet, but coders can alter code and rebuild their bots in fairly short order.
  - The challenge for us, both public and private sector, is to make a lasting impact by criminal or civil action against the coders and herders creating these bots.

Recent Cases

It has been a monumental period for FBI Cyber.

- **Chinese Espionage Case**
  - On Monday, May 19, 2014, an indictment was unsealed in the Western District of Pennsylvania **charging five members of the People's Liberation Army of the People's Republic of China with 31 counts of computer hacking, economic espionage, and other offenses**
  - FBI subjects Wang Dong, Sun Kailiang, Wen Xinyu, Huang Zhenyu, and Gu Chunhui were officers of the Peoples Republic of China, Third Department of the General Staff Department of the Peoples Liberation Army (3PLA), Second Bureau, Third Office, Military Unit Cover Designator (MUCD) 61398 ("Unit 61398") at some point during the investigation
  - As alleged in the indictment, each individual provided their individual expertise to a conspiracy to penetrate the computer networks of six U.S. companies while those companies were engaged in negotiations, joint ventures, or pursuing legal action with or against state-owned enterprises in China
  - **Victim companies include**: Westinghouse Electric Co., SolarWorld, U.S. Steel Corp., Allegheny Technologies Inc., the United Steel, Paper and Forestry, Rubber, Manufacturing, Energy, Allied Industrial and Service Workers International Union and Alcoa Inc.

- **Blackshades Takedown**
  - On Monday, May 19, 2014, FBI New York announced a number of law enforcement actions related to the investigation of the company Blackshades
  - Blackshades sold and distributed malicious software to thousands of individuals throughout the world
  - Blackshades' flagship product was the Blackshades Remote Access Tool (the "RAT"), a sophisticated piece of malware that enabled its users to remotely and surreptitiously gain complete and total control over a victim's computer

- Once installed on a victim's computer, a user of the RAT was free to, among other things, access and view documents, photographs and other files on the victim's computer, record all of the keystrokes entered on the victim's computer, and even activate the web camera on the victim's computer - all of which could be done without the victim's knowledge
- We **believe the RAT was purchased** by **thousands** of people in **over 100 countries** and used to **infect more than 700,000 computers** in **more than 100 countries**

- **<u>GameOver Zeus Takedown</u>**
  - On Monday, June 2, Executive Assistant Director Anderson participated in a press conference at the Department of Justice announcing a string of separate indictments of overseas cyber criminals who brazenly used technology to steal money and property from individuals and companies in the U.S. and around the world
  - Charges were announced against a Russian citizen, Evgeniy Bogachev (Yev-GHEN-ee-BO-ga-chev] as the administrator of both the GameOver Zeus botnet and Cryptolocker malware, the main guy behind the keyboard
  - The malicious software that comprises Gameover Zeus can be used to steal banking credentials, which facilitates the illegal withdrawal of funds from individuals and businesses through financial institutions. The criminals' ability to access accounts at will undermines business integrity and public confidence and has the potential to threaten financial infrastructure
  - **GameOverZeus is the most sophisticated botnet the FBI and our allies have ever attempted to disrupt.** We could not have done it without our partners in the private sector, international law enforcement, and the USG
  - Security researchers **estimate there could be approximately 500,000 to 1 million infections around the world**, and approximately 25 percent of the infected computers are located in the United States
  - The **FBI estimates that Gameover Zeus is responsible for more than $100 million in losses**

What is the FBI doing about the threat?

- **The good news:**
  - Lessons learned from 9/11:
    - Early collaboration between interagency is essential.
    - Information sharing domestically and internationally with ICs, government agencies and private sector is key for a full-scope assessment of the threat.

- **FBI/Government Response & Collaboration**
  - Due to the pervasiveness of the threat, and its impact across all programs, there are a lot of agencies with cyber responsibilities.
  - Coordinated Response – **First Look**
  - USIC coordinates notification, so the private sector entity is not contacted multiple times with the same information.
  - Our CTFs invite USSS to join on all notification calls.
  - Interagency, sector-specific briefings, in advance of potential attacks.
  - Advance notification & briefings to financial sector for DDOS.
  - *Recent Financial Sector briefings* ***UNCLASS ENVIRONMENT.***
  - Proactive notification through briefings and reports.

- **Private Sector Engagement**
  - **Unique benefits to establishing partnerships with FBI *before* cyber incidents occur:**
    - Federal law enforcement agencies work with their USIC partners as well as domestic and international agencies to identify emerging threats and determine tactics and techniques of cyber adversaries.
      - The FBI can provide information as to who is targeting certain companies (nation state v. criminal entities), what the methodology is behind the operations (CNA vs. CNE), patterns of activities, and the motives behind the nefarious acts.
      - Although FBI cannot provide advice on how to protect a company's cyber infrastructure, they can provide the necessary background information on the threats and threat actors so that industry can make informed decisions on how best to protect their networks.
      - Establishing and exercising incident response plans which include both government and private sector also identifies gaps that need to be addressed in order to effectively battle cyber adversaries.
    - Although there may be a belief by private industry that computer intrusions are a 'necessary evil' that every company must deal with, the FBI and the USIC have valuable information regarding threat actors and certain patterns of activity.
      - What may seem like insignificant activity to a company may be the missing puzzle piece needed to deter a large scale attack.
      - The FBI is in the unique position to collect both investigative information and intelligence regarding cyber matters which are ultimately used to identify TTPs, patterns, and emerging threats.

  - By opening lines of dialogue and encouraging information sharing, both private industry and government agencies demonstrate to the American public that there is a whole-of-nation approach in dealing with cyber threats.
- Working with the FBI does not necessarily mean that the collaboration will lead to an investigation.
  - The FBI coordinates with each individual company to determine the best course of action to address the incident. In some instances, neutralizing the threat may the best option in lieu of a law enforcement action.
  - No matter what course of action is deemed appropriate, information provided by a victim or a *potential* victim is protected.
- Informing the FBI of intrusions or potential intrusions provides an opportunity for the federal government to surge its capabilities in addressing the malicious activity. These resources, along with an over view of cyber threats and what we are doing to address them is the theme of my discussion today.

- When it comes to public-private partnerships and information sharing, we are shifting from a reactive to a stronger proactive posture.
- Whole of government approach
- Bringing USIC and international partners into the NCIJTF
- 19 agencies – focused on investigative collaboration
- Coordinated outreach and briefings to private sector
- Leverage existing relationships
- **InfraGard**- Currently 23,000+ active members
- **DSAC** - The Domestic Security Alliance Council is a strategic partnership between the U.S. Government (USG) and U.S. Private Industry.
  - Its goal is to increase security by enhancing communications and promoting the timely and effective exchange of security information among its constituents.
  - Advances the FBI's mission of preventing, detecting, and deterring criminal acts by facilitating strong, enduring relationships among its private industry members, FBI Headquarters (FBIHQ) divisions, FBI field offices, Department of Homeland Security (DHS) Headquarters, DHS Fusion Centers, and other Federal Government entities.
- **Cyber Sector-specific outreach – Key Partnership Engagement Unit**
  - CyD partnership program with c-suite level managers.
- Building Guardian- Portal/Pipeline for industry

Cyber Division Talking Points

- **NCFTA** - National Cyber-Forensics & Training Alliance
  - Embedding of FBI personnel through **CIRFU** (Cyber Initiative and Resource Fusion Unit) to collaborate on combating cyber crime
  - **Malware Investigator API** deployed to NCFTA for Malware Analysis
- Machine-to-Machine, real time Information sharing
  - Building an Automated, **2-way Exchange** for threat information
- Discretion to Prosecute
- Partnering with Private Industry to Identify, Pursue and Defeat the Adversary