Agency Priority Goal Action Plan

Combat Cyber-Enabled Threats and Attacks

Goal Leader:

Jolene Lauria, Deputy Assistant Attorney General/Controller

Performance.gov

Fiscal Year 2018, Quarter 3

Overview

Goal Statement

- Cybercrime is of one of the greatest threats facing our country, and has enormous implications for our national security, economic prosperity, and public safety. The range of threats and challenges cybercrime presents for law enforcement expands just as rapidly as technology evolves. By September 30, 2019, the Department of Justice will combat cyber-enabled threats and attacks by conducting 8,400 computer intrusion program deterrences, detections, disruptions and dismantlements, while successfully resolving 90 percent of its cyber defendant cases. FY 2018 will serve, as a baseline for FBI's "number of computer intrusion programs" measure.

• Challenges

- More and more sensitive data stored online, may increase the number of cyber targets, threats and attacks on U.S. computers and networks.
- More sophisticated cyber defendants may pose increased threats.

• Opportunities

- Eliminating the capabilities of a threat enterprise/organization engaged in criminal or national security related activities.
- Deterring, detecting, disrupting, and dismantling, or incapacitating cyber threat actors and computer intrusion programs by prosecuting cyber defendant cases.

Leadership and Partners

Core Leadership Team:

- Federal Bureau of Investigations (FBI)
- National Security Division (NSD)
- United States Attorneys' Offices (USAO)
- Criminal Division (CRM)

Other Participating Components:

- Organized Crime Drug Enforcement Task Forces (OCDETF)

Stakeholders:

- Community and business leaders

Goal Structure & Strategies

To combat cybercrime, the Department will increase the number of computer intrusion programs deterred, detected, disrupted and dismantled; and resolve at least 90 percent of defendants' cases in the Department's favor.

Strategy: Identify, disrupt, and prosecute cyber threat actors.

- The Department will charge individuals acting on behalf of nation-states to harm our national interests, transnational organized crime groups, and individuals for launching cyber attacks against computers in the United States.

Strategy: Develop and use all appropriate tools to identify and disrupt cyber threats.

- To attribute and disrupt attacks, the Department will continue its collaboration with other agencies, including the intelligence and defense communities, to aid attribution and ensure that responses are both effective and consistent with law.

Summary of Progress – FY 18 Q3

The Combat Cyber-Enabled Threats and Attacks tracks two performance measures. Both measures have quarterly targets. Of the two measures, only one exceeded its target for Q3 FY 2018.

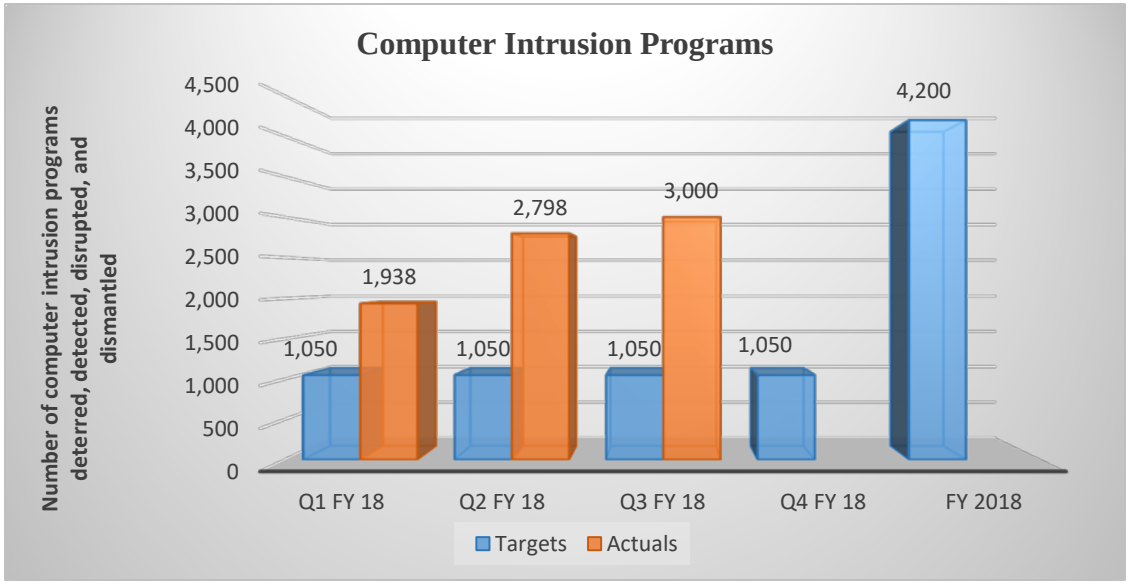
- For Q3, FBI exceeded its quarterly target of 1,050, by nearly 2,000 for the number of computer intrusion programs deterred, detected, disrupted and dismantled. Since Q1, FBI has greatly exceeded its quarterly targets. To date, the total number of computer programs affected is 7,736 – 84% more than the annual target of 4,200.
- For Q3, only 80% of the Department's cyber defendants cases were favorably resolved. Since Q1, the Department continues to slightly miss its quarterly target of 90%.

  As with all cases handled by the Department, each was individually evaluated throughout the judicial process, including the decision to initiate charges. The Department will continue to individually assess each case brought for criminal prosecution in a manner that promotes the ends of justice. While the Department may meet its Q4 target, it is not on track to meet the annual target for this measure.

Performance Measures

Performance Measure: Number of computer intrusion programs deterred, detected, disrupted and dismantled [FBI]

Progress Updates – Q3



- In previous years, FBI's Cyber Division measured only the number of disruptions and dismantlements.

- Number of computer intrusion programs deterred, detected, disrupted and dismantled is a new measure reported by FBI's Cyber Division, quarterly and annually. FY 2018, will serve as a baseline for this measure.

- For Q3 FY 2018, FBI exceeded its quarterly target of 1,050, by nearly 2,000 programs. To date, the cumulative number of computer intrusion programs deterred, detected, disrupted and dismantled is 7,736 – 84% more than the annual target.

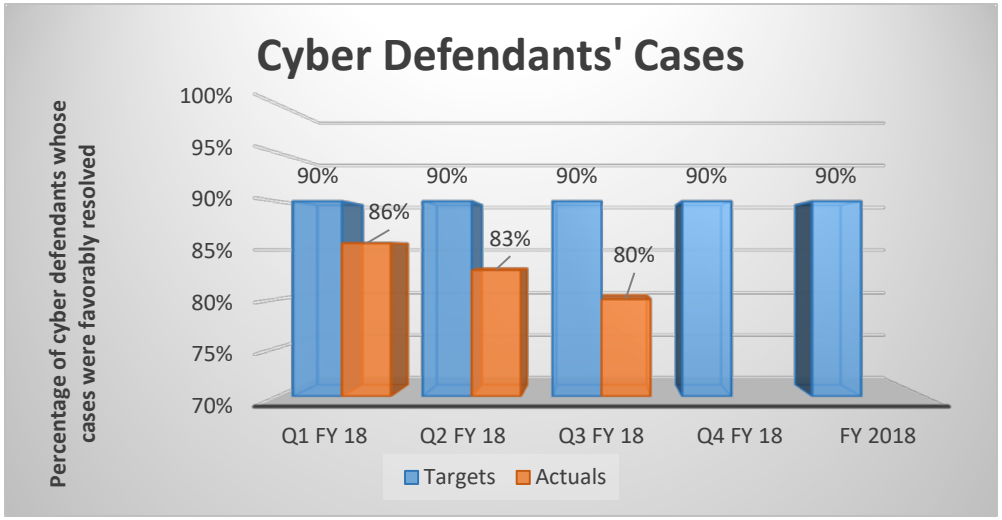
Performance Measures

Performance Measure: Percentage of cyber defendants whose cases were favorably resolved [USAO, CRM and NSD]

Historical Data

Fiscal Years	Actuals
FY 2015	100%
FY 2016	100%
FY 2017	100%

Progress Updates – Q3



- USAO, NSD and CRM will report the data for this measure, quarterly and annually.

- For Q3 FY 2018, the Department favorably resolved 105 of 131 cyber cases (80%), short of achieving the target for the quarter (90%). As with all cases handled by the Department, each was individually evaluated throughout the judicial process, including the decision to initiate charges. Depending upon the total number of cases resolved during any given quarter, a one case differential can significantly impact the favorable percentage.

- Many cases concerning "cybercrime" may not necessarily be captured under this number, as there is not a single statute to prosecute criminal cyber conduct. Cyber cases tend to involve other related criminal conduct under which the matter could be coded in the EOUSA case management database. USAOs will continue to individually assess each case brought for criminal prosecution in a manner that promotes the ends of justice.

Data Accuracy and Reliability

There are two key performance indicators for the Cybercrime priority goal.

- **Number of computer intrusion programs deterred, detected, disrupted and dismantled.** This measure is reported by the FBI's Cyber Division. The FBI proposed a new metric, "Deter, Detect, Disruptions, and Dismantlements" in order to capture data that most appropriately measures FBI's actions against cyber adversaries.

    - A disruption is defined as interrupting or inhibiting a threat actor from engaging in criminal or national security related activity. The proliferation of synthetic drugs requires additional analytical resources in order to accurately identify and schedule the compounds.
    - Dismantlement means that the targeted organization's leadership, financial base and supply network has been destroyed, such that the organization is incapable of operating and/or reconstituting itself.

The FBI Cyber Division's operational priorities are classified. Therefore, only aggregate data that lacks significant detail can be publicly reported. Data is collected routinely and stored on a classified enterprise platform. Data is validated and verified manually. FY 2018, will serve as a baseline year for this measure.

- **Percentage of cyber defendants whose cases were favorably resolved.** This measure will be reported by NSD, CRM, and USAO. Defendants whose cases were favorably resolved include those defendants whose cases resulted in court judgements favorable to the government.

  Data validation and verification is accomplished by the following:

    - NSD's Counterterrorism Section and the Counterespionage Section reviews quarterly data.

Data Accuracy and Reliability Cont.

- USAOs routinely examine current and historical data sets, as well as look for trends to ensure the data are as accurate and reliable as possible and targets are ambitious enough given the resources provided. USAOs also maintain the accuracy and integrity of the statistical data maintained in the Legal Information Online Network System, which contains information on matters, cases, and appeals handled by the USAOs, and the companion USA-5 reporting system, which tracks how USAO personnel spend their time. The data is reviewed by knowledgeable personnel; attorneys and support personnel are responsible for ensuring the local procedures are followed for maintaining the integrity of the data in the system.

- CRM captures all litigation data in its Automated Case Tracking System (ACTS). Data in ACTS is validated quarterly by Computer Crime and Intellectual Property Section's (CCIPS) Section Chief.