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 4

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 End-of-Year

The Combat Cyber-Enabled Threats and Attacks tracks two performance measures. Both measures have quarterly targets, and both measures exceeded their targets for FY 2018.

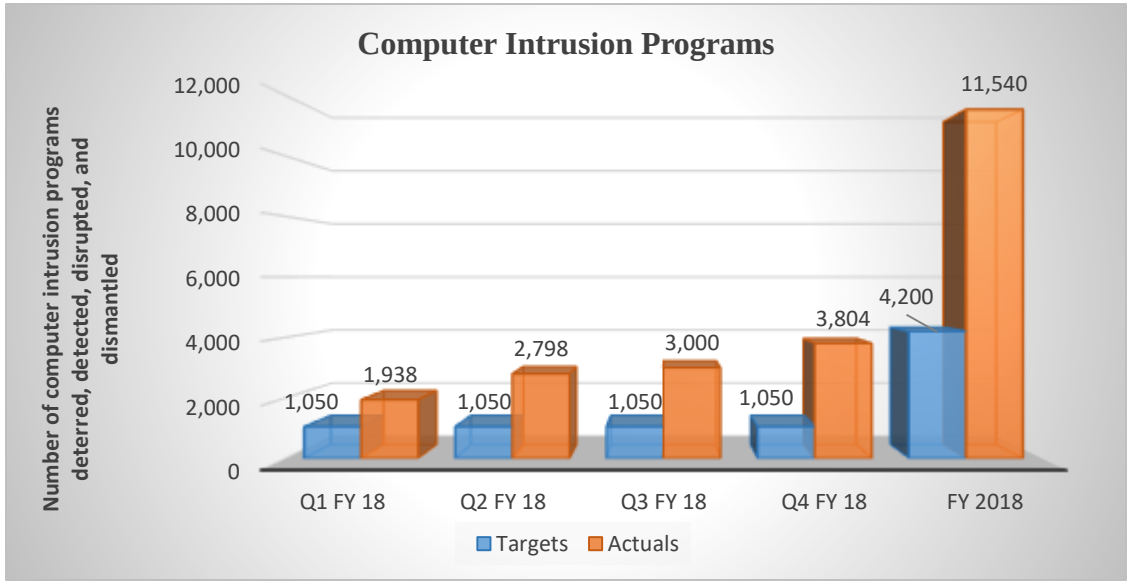
- By the end of FY 2018, FBI exceeded its annual target of 4,200, by 7,340 for number of computer intrusion programs deterred, detected, disrupted and dismantled. Throughout the year, FBI greatly exceeded its quarterly targets. The total number of computer programs affected was 11,540 – more than double the annual target for FY 2018.

- For FY 2018, the Department favorably resolved 157 of 160 cyber cases (98%), exceeding the annual target (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, 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 Executive Office for U.S. Attorneys' case management database. U.S. Attorneys will continue to individually assess each case brought for criminal prosecution in a manner that promotes the ends of justice.

Performance Measures

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

Progress Updates – Q4/End-of-Year



- 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 Q4 FY 2018, FBI exceeded its quarterly target of 1,050, by nearly 2,754 programs. The cumulative number of computer intrusion programs deterred, detected, disrupted and dismantled is 11,540 – more than double the annual target.

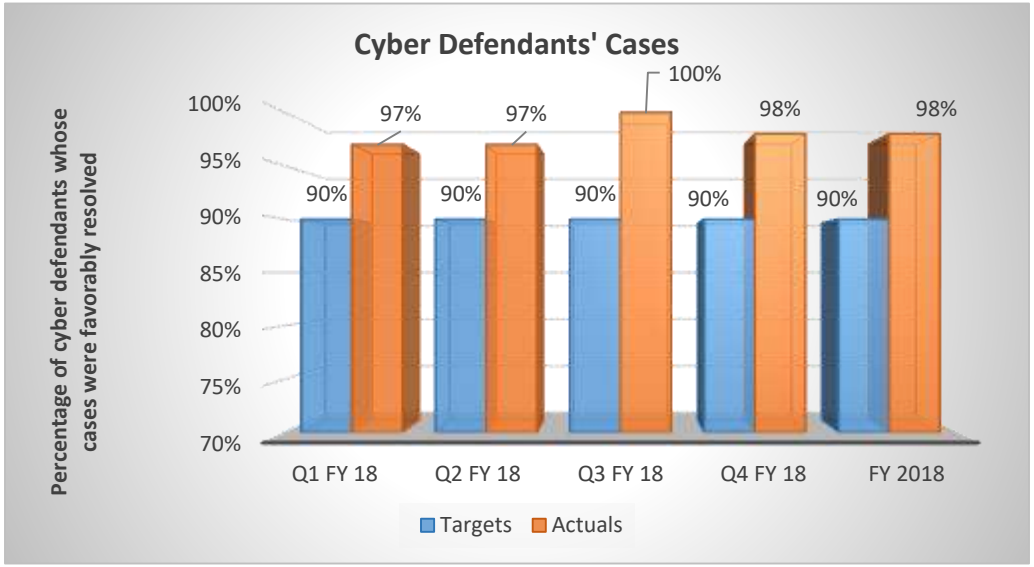
Performance Measures

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 – Q4/End-of-Year



*The quarterly and annual results for this measure have been updated since last reported.

- USAO, NSD and CRM will report the data for this measure, quarterly and annually.
- For Q4, 98% of the 42 cyber cases handled by the Department were favorably resolved. For FY 2018 in total, the Department favorably resolved 157 of 160 cyber cases (98%), exceeding the annual target (90%).

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.
    - 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 judgments favorable to the government, such as convictions after trial or guilty pleas. Unfavorable dispositions include not guilty verdicts. Cases dismissed based on government-endorsed motions were not categorized as either favorable or unfavorable for purposes of this calculation. Such motions may be filed for a variety of reasons to promote the interest of justice.

Data Accuracy and Reliability Cont.

As with all cases handled by USAOs, each was individually evaluated throughout the judicial process, including the decision to initiate charges. By way of example, in the assessment of an individual case, a USAO may choose to dismiss felony charges for various reasons, including, but not limited to, dismissal of a felony charge(s) in lieu of a defendant's negotiated plea to a misdemeanor charge(s), or dismissal of an indictment in order to conserve government resources due to the inability of law enforcement to locate overseas individuals for arrest despite lengthy attempts to do so. USAOs will continue to individually assess each case brought for criminal prosecution in a manner that promotes the ends of justice.

Data validation and verification is accomplished by the following:

- NSD's Counterintelligence and Export Control Section reviews quarterly data.

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

- USAO data is entered locally by each district, where district personnel (attorneys and support staff) are responsible for ensuring procedures are followed to maintain the integrity of data in the system. Data is collectedly nationally in CaseView (formerly, the Legal Information Online Network System), which contains information on matters, cases, and appeals handled by all USAOs. The companion USA-5 reporting system tracks how USAO personnel spend their time. That data is reviewed by knowledgeable personnel, including data analysts and others. Case statistics for purposes of the instant analysis were compiled by the Executive Office for United States Attorneys (EOUSA) using the case management database.

Data Accuracy and Reliability Cont.

Many cases concerning “cybercrime” may not necessarily be captured under these statistics, 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 database. USAOs routinely examine current and historical data sets, as well as look for trends to ensure that the data is as accurate and reliable as possible and targets are ambitious enough given the resources provided.

Depending upon the total number of cases resolved during any given quarter, a one case differential can significantly impact the favorable percentage.