Agency Priority Goal Action Plan

Combat Cyber-Enabled Threats and Attacks

Goal Leader(s):

Sujit Raman
Associate Deputy Attorney General
Office of the Deputy Attorney General

Performance.gov

Fiscal Year 2020, Quarter 3

Overview

Goal Statement

- Cybercrime is 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, 2021, the Department of Justice will combat cybercrime threats and attacks by conducting 16,000 computer intrusion program deterrences, detections, disruptions and dismantlements; favorably resolving 90 percent of prosecutions of cyber defendants; and increasing the percentage of private sector losses recovered by the FBI's Internet Crime Complaint Center (IC3) to 78 percent. The results from FY 2018 (73%) currently serve as a baseline for the Department's new IC3 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, dismantling, or incapacitating cyber threat actors and computer intrusion programs by prosecuting cyber defendant cases.
- Improving the likelihood of recovering losses from illicit actors and activities by building stronger partnerships with key private sector institutions.

Leadership & Implementation Team

Core Leadership Team

- Federal Bureau of Investigations (FBI)
- National Security Division (NSD)
- United States Attorneys’ Offices (USAO)
- Criminal Division (CRM)
- Office of Legal Policy (OLP)
- Office of the Deputy Attorney General (ODAG)

Stakeholders

- Consumers (Data privacy & security, availability of data, data integrity)
- Businesses (Data privacy & security, availability of data, data integrity)
- Government Entities (Critical infrastructure protection, national security and law enforcement, data integrity)
- Community leaders

Goal Structure & Strategies

STRATEGIES	GOALS	RISKS
<u>Strategy 1</u>: Identify, disrupt, and prosecute cyber threat actors • The Department will charge or otherwise disrupt individuals acting on behalf of nation-states to harm our national interests; transnational organized crime groups; and individuals launching cyber-attacks against computers in the United States.	• The Department exceeded its two-year target for the FY 2018 - 2019 Cyber Priority Goal, by favorably resolving 99% of its prosecutions of 325 cyber defendants. • Goal: The Department will continue to work to favorably resolve at least 90 percent of its prosecutions of cyber defendants. ➢ Performance Indicator: Percentage of prosecutions of cyber defendants that were favorably resolved	▪ Lawful access (formerly Going Dark) ▪ Case Locations (cyber threats continue to expand beyond major cities across the nation) ▪ Sophistication of Cyber Threats ▪ Private Sector Engagement
<u>Strategy 2:</u> 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 the law.	• The FBI’s Cyber Division exceeded its two-year target for the FY 2018 - 2019 Cyber Priority Goal, by deterring, detecting, disrupting and dismantling a total of 27,437 computer intrusion programs. • Goal: By FY 2021, the FBI will continue with its strategy and conduct at least 16,000 computer program intrusion investigations. ➢ Performance Indicator: Number of computer intrusion programs deterred, detected, disrupted and dismantled	

Goal Structure & Strategies

STRATEGIES	GOALS	RISKS
Strategy 3: Strengthen public-private partnerships • The Department will continue its efforts to build trust with key private sector institutions. The FBI's Internet Crime Complaint Center (IC3) will continue to perform outreach and educate victims on filing with IC3 in a complete and timely manner, as domestic transfers are quickly dispersed. • IC3 will continue to partner with regulators to monitor the effects of legal guidance that influence financial sectors' ability to recover fraudulent funds.	• In FY 2019, the FBI developed a new measure that better demonstrates how it proactively improves the likelihood of losses recovered from illicit actors and activities, through its efforts to work with private institutions. The IC3 was established in FY 2018. Each year, the FBI's IC3 will increase the percentage of private sector losses recovered. • Goal: By FY 2021, the FBI's IC3 will increase the percentage of losses recovered from 73 percent, to 76 percent. ➢ Performance Indicator: Percentage of private sector losses recovered by the FBI's Internet Crime Complaint Center (IC3)	

Summary of Progress – FY 20 Q3

The FY 2020 – 2021 Combat Cyber-Enabled Threats and Attacks Priority Goal tracks three performance measures. The measures track the progress of the three strategies outlined in the previous slides. Each measure has quarterly and annual targets. All measures have exceeded their targets for Q3 FY 2020.

The Cyber Division will continue its coordinated operational activities to disrupt and dismantle as well as detect and deter the top cyber threat actors.

- The FBI exceeded its quarterly targets (2,000) for Q3/FY 2020 – successfully deterring, detecting, disrupting or dismantling a total of 3,719 computer intrusion programs this quarter. To date, the FBI has already achieved 9,847 investigative outcomes – exceeding its annual target (8,000) by 23%.

Cyber cases tend to involve other related criminal conduct which the matter could be coded in the EOUSA case management system.

- The Department exceeded its quarterly targets for Q3/FY 2020 to favorably resolve cyber defendant cases – each of the 12 cases prosecuted in the third quarter of the fiscal year were successful. By the end of Q3, 100% of the 84 cases handled by the Department were successfully resolved.

In FY 2018, the FBI officially established the Internet Crime Complaint Center (IC3). In FY 2019, the IC3 began reporting on the percentage of private sector losses they recovered. The purpose of this new metric is to capture data that measures IC3's ability to recover private sector losses.

- For Q3 FY 2020, the FBI's IC3 exceeded its quarterly target (77%) by successfully recovering 89% of private sector losses this quarter.

For Q3 FY2020, the FBI's results were higher than the projected target due to prompt reporting by victims, and the collaborative relationships established with financial institutions. The FBI's IC3 and Rapid Asset Team (RAT) are confident they will continue to provide services to the private sector, even during the pandemic, and achieve their outcome to increase the percent of private sector losses recovered.

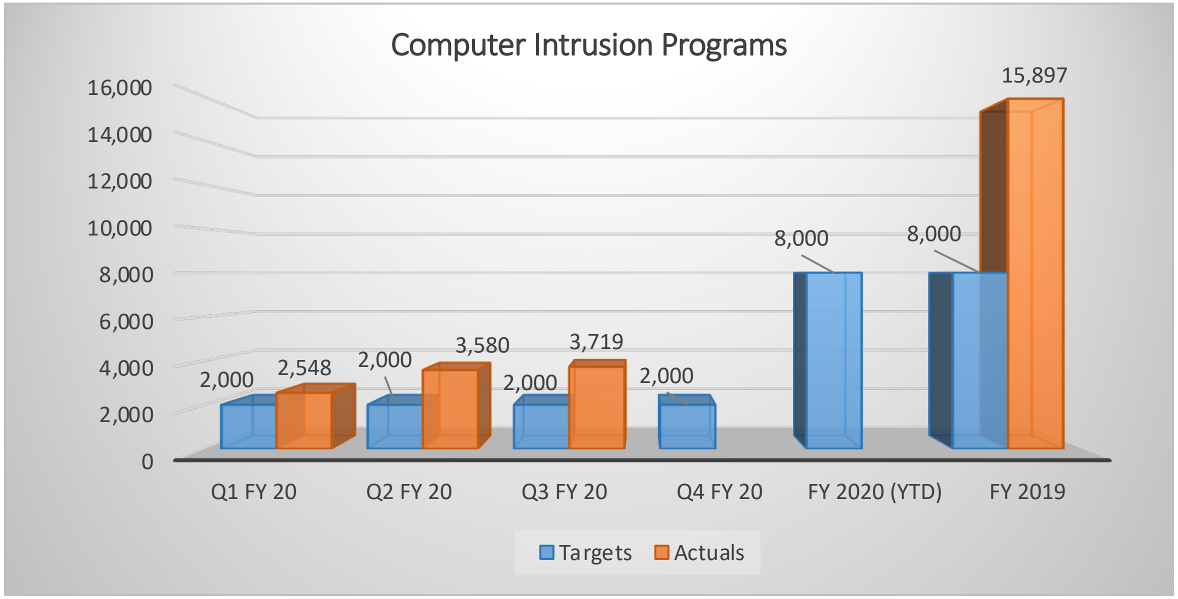
Key Indicators

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

Historical Data

Fiscal Years	Actuals
FY 2018	11,540
FY 2019	15,897

Progress Updates – Q3 FY 2020



- Number of computer intrusion programs deterred, detected, disrupted and dismantled is reported by the FBI's Cyber Division, both quarterly and annually. The FBI began reporting on this measure in FY 2018.

- For Q3 FY 2020, the FBI's Cyber Division exceeded its quarterly target by successfully deterring, detecting, disrupting or dismantling a total of 3,719 computer intrusion programs this quarter. To date, the FBI has already achieved 9,847 investigative outcomes – exceeding its annual target (8,000) by 23%.

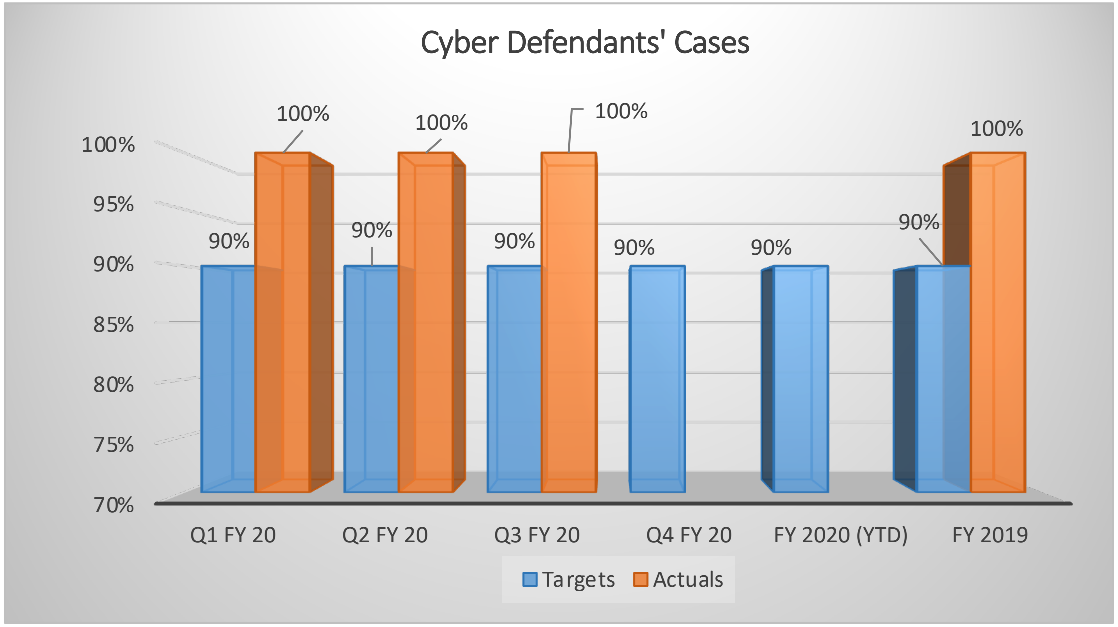
Key Indicators

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

Historical Data

Fiscal Years	Actuals
FY 2015	100%
FY 2016	100%
FY 2017	100%
FY 2018	98%
FY 2019	100%

Progress Updates – Q3 FY 2020



- USAO, CRM and NSD will report the data for Percentage of prosecutions of cyber defendants that were favorably resolved, both quarterly and annually.

- For Q3 FY 2020, the Department prosecuted 12 cyber defendants – each case was resolved favorably. To date, the Department has successfully prosecuted a total of 84 cases.

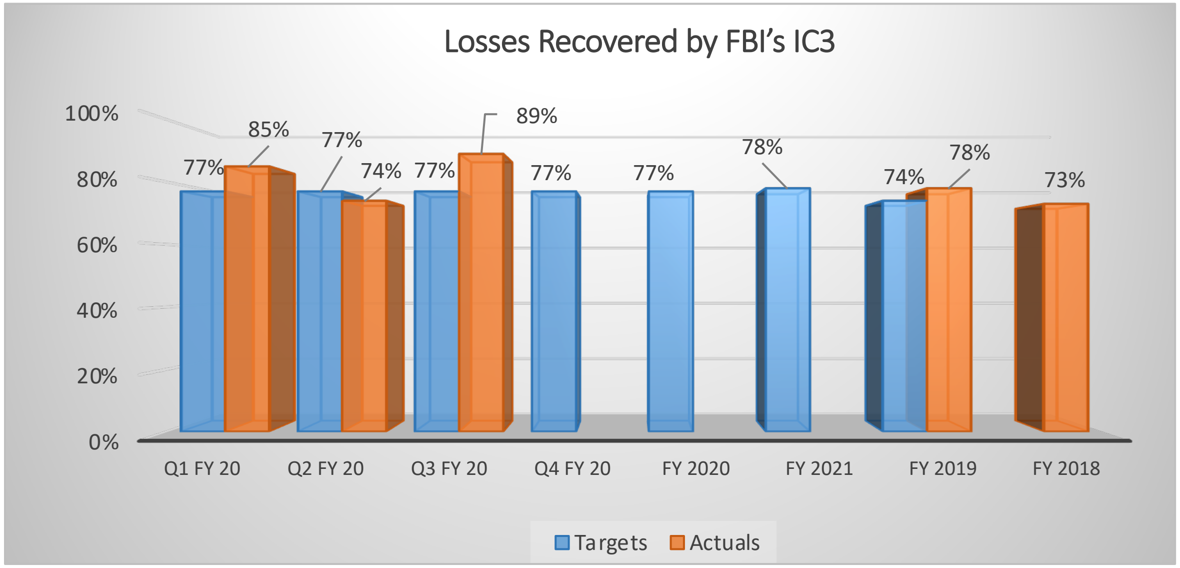
Key Indicators

Performance Measure: Percentage of private sector losses recovered by the FBI's Internet Crime Complaint Center (IC3) [FBI]

Historical Data

Fiscal Years	Actuals
FY 2017	30%
FY 2018 (IC3 established - Baseline)	73%
FY 2019	78%

Progress Updates – Q3 FY 2020



- Percentage of private sector losses recovered is a new measure reported by the FBI's Internet Crime Complaint Center (IC3), that was officially established in FY 2018. The results reported for FY 2018 (73%) will serve as a baseline for the measure.

- For Q3 FY 2020, FBI's IC3 recovered 89% of private sector losses this quarter. FBI's IC3 and Rapid Asset Team (RAT) are confident they will continue to provide services to the private sector, even during the pandemic, and achieve their outcome to increase the percent of private sector losses recovered. The Cyber Division (CyD) highlighted how their IC3 RAT efforts continue to achieve high recoveries, based on trends from the last two to three years. IC3 has been even more visible on the front page of fbi.gov (https://www.fbi.gov/) and other FBI social media posts, in order to get more private sector organizations and individuals to reach out to the IC3.

Data Accuracy and Reliability

There are three 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 this metric in FY 2018, "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.
  - Detect is the FBI identification of a threat actor and/or criminal or national security related activity. The detect should be claimed by the FBI Case Agent when known or suspected personnel, assets, front company/cover organizations, funding, operations, objectives, or tradecraft are detected or identified.
  - Deter is the FBI prevention of a threat actor from engaging in criminal or national security related activity through defensive countermeasures which are implemented by the FBI, or implemented by strategic partners due to FBI engagement. The deterrence should be claimed by an Agent when the Agent's defensive countermeasures were implemented by the FBI or implemented by strategic partners due to FBI engagement.

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.

- **Percentage of private sector losses recovered by the FBI's Internet Crime Complaint Center (IC3).** This measure is reported by the FBI's Internet Crime Complaint Center (IC3).

The FBI proposed this new metric in FY 2019, in order to capture data that measures its ability to recover private sector losses. The nation's cyber infrastructure is overwhelmingly managed and controlled by the private sector, and efforts to protect it, therefore, involve robust cooperation and information sharing with those partners. This measure addresses one of the Department's key strategies, in both the strategic plan and Cyber APG, to strengthen public-private partnerships.

- The FBI's Rapid Asset Team (RAT) defines a loss as funds diverted from a victim's account to a fraudulent recipient account via deception techniques employed by fraud actors. A "recovered loss" is defined as funds frozen, or held, at the recipient financial institution and unable to be retrieved by the bad actor. Since the foundation of the IC3
- The FBI proposed this new metric in FY 2019, in order to capture data that measures its ability to recover private sector losses. The nation's cyber infrastructure is overwhelmingly managed and controlled by the private sector, and efforts to protect it, therefore, involve robust cooperation and information sharing with those partners. This measure addresses one of the Department's key strategies, in both the strategic plan and Cyber APG, to strengthen public-private partnerships. For more information about the IC3, go to ic3.gov.
- Since the IC3' RAT was officially established in FY 2018, the results of that year will serve as a baseline for this measure.

Since the IC3 was officially established in FY 2018, the results of that year will serve as a baseline for this measure.