GAO Highlights

Highlights of GAO-23-106080, a report to congressional committees

June 2023

CYBERCRIME

Reporting Mechanisms Vary, and Agencies Face Challenges in Developing Metrics

Why GAO Did This Study

Cybercrime (including cyber-enabled crime) generally consists of criminal activities that target a computer or network for damage or infiltration or use the internet to conduct criminal activity. Cybercrime in the United States is increasing, resulting in billions of dollars in losses and threatening public safety. However, the United States lacks comprehensive cybercrime data and monitoring, leaving the country less prepared to combat cybercrime. The Better Cybercrime Metrics Act, enacted in 2022, requires DOJ to develop a taxonomy for types of cybercrime and cyber-enabled crime and establish a category in its National Incident-Based Reporting System to collect reports for cybercrime from law enforcement. The act also includes a provision for GAO to report on existing cybercrime reporting mechanisms.

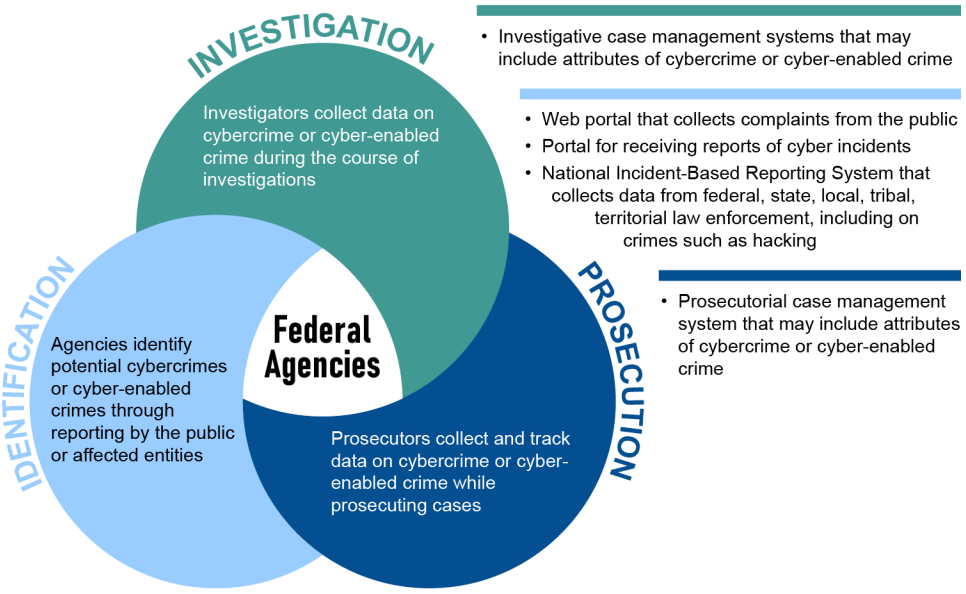
The objectives of this review were to focus on (1) existing mechanisms used to report cybercrime and cyber-enabled crime, including reported strengths and limitations; (2) differences between data reported on cybercrime or cyber-enabled crime and other types of crime; and (3) challenges selected agencies reported in defining shared metrics for cybercrime. GAO identified agencies with key responsibilities for identifying, investigating, and prosecuting cybercrime. GAO reviewed documentation on agency mechanisms for reporting cybercrime data, such as case management systems. It also interviewed agency officials regarding these mechanisms, differences between cybercrime and other types of crime, and challenges in establishing shared metrics.

View GAO-23-106080. For more information, contact Marisol Cruz Cain at (202) 512-5017 or cruzcainm@gao.gov or Gretta L. Goodwin at (202) 512-8777 or goodwing@gao.gov.

What GAO Found

Federal agencies use a variety of mechanisms to collect and report data on cybercrime. The mechanisms used depend on whether the agency's mission related to cybercrime is identification, investigation, or prosecution. (See figure.)

Types of Agency Mechanisms Used for Reporting Cybercrime



Source: GAO analysis of agency information. | GAO-23-106080

Note: GAO identified 12 agencies, including the Department of Justice, Federal Bureau of Investigation, and Internal Revenue Service; the entire list is included in the report.

Strengths of these mechanisms included specific functionality for capturing cybercrime attributes to facilitate information sharing. Limitations included variations in how systems classify and track cybercrime and the absence of a central mechanism that collects data on cybercrime. These are partly due to the lack of an official or commonly agreed-on definition of cybercrime.

Agencies also identified differences between data reported on cybercrime (including cyber-enabled crime) and other types of crime. For example, cybercrime may not be consistently tracked because it is not always associated with a specific type of offense. In addition, victims may be hesitant to report cybercrime because of lack of familiarity or reputational concerns.

Agencies identified challenges in defining shared metrics. These include measuring the extent and impact of cybercrime, agreeing on a definition of cybercrime, and coordinating among law enforcement agencies at various levels. The Department of Justice (DOJ) effectively developing a cybercrime taxonomy and category in its national crime reporting system should help address these challenges. GAO intends to monitor future efforts, including those to develop cybercrime categories and ensure consistent reporting.