United States Government Accountability Office

Report to Congressional Committees

June 2023

CYBERCRIME

Reporting Mechanisms Vary, and Agencies Face Challenges in Developing Metrics

GAO-23-106080

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.

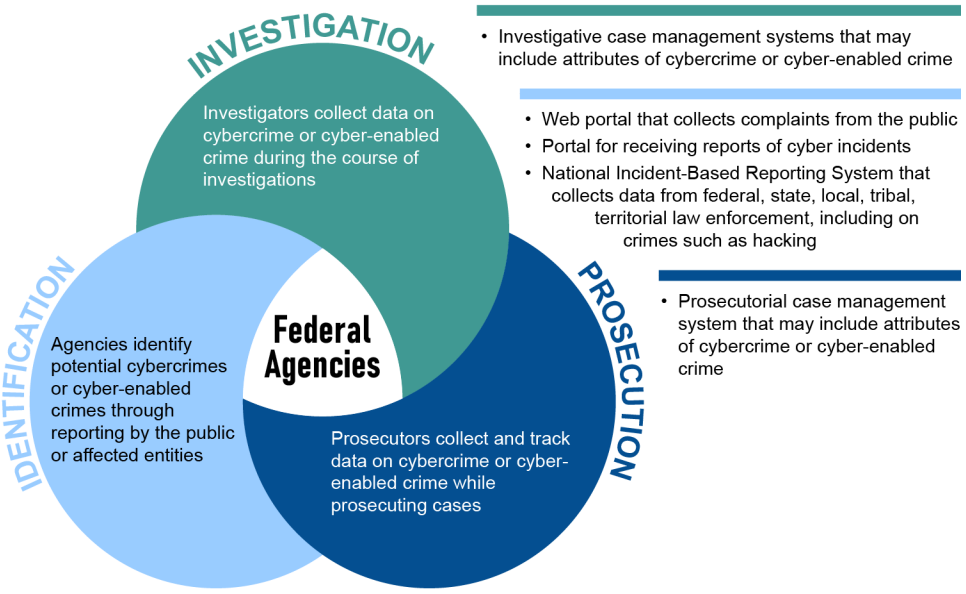
The objectives of this review were to focus on (1) existing mechanisms used to report cybercrime and cyber-enabled crime, including reported strengths and limitations; (2) differences between data reported on cybercrime or cyber-enabled crime and other types of crime; and (3) challenges selected agencies 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.

Contents

Letter		1
	Background	4
	Agencies Use Various Mechanisms to Report Cybercrime and Noted Strengths and Limitations	11
	Agencies Noted Differences between Reporting Cybercrime and Other Crimes	23
	Agencies Identified Challenges in Establishing Cybercrime Metrics	25
	Agency Comments	30
Appendix I	Objectives, Scope, and Methodology	32
Appendix II	GAO Contacts and Staff Acknowledgments	35
Tables		
	Table 1: Cybercrime-Related Responsibilities of Selected Agencies	6
	Table 2: Selected GAO Reports Addressing Aspects of Cybercrime and Cyber-Enabled Crime	9
Figures		
	Figure 1: Types of Mechanisms Agencies in Our Review Used for Reporting Cybercrime	12
	Figure 2: Functionality That Selected Agency Systems Used to Collect Cybercrime-Related Data	20
	Figure 3: Challenges in Establishing Cybercrime Metrics	26

Abbreviations

ATF	Bureau of Alcohol, Tobacco, Firearms, and Explosives
BJS	Bureau of Justice Statistics
CCIPS	Computer Crime and Intellectual Property Section
CISA	Cybersecurity and Infrastructure Security Agency
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DOJ	Department of Justice
FBI	Federal Bureau of Investigation
FIRS	Field Investigative Reporting System
FinCEN	Financial Crimes Enforcement Network
HSI	Homeland Security Investigations
IC3	Internet Crime Complaint Center
IC3Net	IC3 Network
IRS	Internal Revenue Service
NIBRS	National Incident-Based Reporting System
NSD	National Security Division
SLTT	state, local, tribal, and territorial
USPIS	U.S. Postal Inspection Service

U.S. GOVERNMENT ACCOUNTABILITY OFFICE
441 G St. N.W.
Washington, DC 20548

June 20, 2023

The Honorable Dick Durbin
Chairman
The Honorable Lindsey Graham
Ranking Member
Committee on the Judiciary
United States Senate

The Honorable Jim Jordan
Chairman
The Honorable Jerrold Nadler
Ranking Member
Committee on the Judiciary
House of Representatives

Cybercrime generally includes criminal activities that specifically target a computer or network for damage or infiltration or use computers as tools to conduct criminal activity. In addition, “cyber-enabled” crime can refer to a variety of traditional criminal acts, such as theft or fraud, which are carried out over the internet. These types of crimes in the United States are increasing and have resulted in hundreds of billions of dollars in losses, threatening public safety and economic security.

Multiple federal agencies have responsibilities to protect against, detect, investigate, and prosecute cybercrime. For example, the Departments of Justice (DOJ) and Homeland Security (DHS) have prominent roles in addressing cybercrime within the federal government. State and local law enforcement entities play similar roles at their levels. However, Congress and researchers have found that the United States lacks comprehensive cybercrime data and monitoring, leaving the country less prepared to combat the cybercrime threatening national and economic security.

The Better Cybercrime Metrics Act, enacted May 5, 2022, includes a provision for GAO to report on the effectiveness of reporting mechanisms for cybercrime and cyber-enabled crime in the United States. It also asks

us to review disparities in reporting data between those relating to cybercrime and cyber-enabled crime and other types of crime data.[1]

The objectives of this review were to identify (1) the existing mechanisms used to report cybercrime and cyber-enabled crime in the United States and the strengths and limitations that have been reported in these mechanisms, (2) the differences between data reported on cybercrime or cyber-enabled crime and other types of crime, and (3) the challenges selected agencies reported in defining shared metrics for tracking cybercrime and cyber-enabled crime in the United States.

We focused this review on selected federal agencies with responsibilities related to cybercrime. We identified key agencies with responsibilities for identifying, investigating, and prosecuting cybercrime based on a review of previous GAO work in this area[2] and by consulting internal GAO stakeholders with subject-matter expertise. We also solicited input from agencies we spoke with to identify additional agencies or offices that play a role in collecting data related to cybercrime. As a result of this selection, we focused our review on the following agencies:

Department of Homeland Security

- United States Secret Service
- Cybersecurity and Infrastructure Security Agency
- Immigration and Customs Enforcement's Homeland Security Investigations

Department of Justice

[1]Better Cybercrime Metrics Act, Pub. L. No. 117–116, § 6, 136 Stat. 1180, 1181 (May 5, 2022) (34 U.S.C. § 30109 note).

[2]See, for example, GAO, *Virtual Currencies: Additional Information Could Improve Federal Agency Efforts to Counter Human and Drug Trafficking*, GAO-22-105462 (Washington, D.C.: Dec. 8, 2021); *Cyberspace: The United States Faces Challenges in Addressing Global Cybersecurity and Governance*, GAO-10-606 (Washington, D.C.: July 2, 2010); and *Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats*, GAO-07-705 (Washington, D.C.: June 22, 2007).

- Federal Bureau of Investigation (including its Baltimore field office,[3] Criminal Justice Information Services Division, and Internet Crime Complaint Center)
- Drug Enforcement Administration
- Bureau of Alcohol, Tobacco, Firearms, and Explosives
- Computer Crime and Intellectual Property Section
- National Security Division
- Bureau of Justice Statistics

Department of the Treasury

- Internal Revenue Service-Criminal Investigation
- Financial Crimes Enforcement Network

U.S. Postal Service

- U.S. Postal Inspection Service[4]

To address our first objective, we reviewed relevant federal laws, including the Better Cybercrime Metrics Act and the Uniform Federal Crime Reporting Act of 1988.[5] In addition, we reviewed agency policies, procedures, and other documentation on processes for collecting, tracking, sharing, and reporting data on cybercrime and cyber-enabled crime. We also reviewed documentation for systems (e.g., databases and case management systems) used by agencies to collect, track, share, and report data on cybercrime and cyber-enabled crime. Lastly, we interviewed cognizant agency officials about their processes and mechanisms for collecting and reporting data on cybercrime and cyber-enabled crime, including the strengths and limitations of existing reporting mechanisms.

To address our second objective, we reviewed agency policies, procedures, and documentation. Further, we reviewed relevant reports from GAO and others, as well as other literature. We also interviewed

[3]We met with the FBI's Baltimore Field Office to understand how FBI field personnel may collect and report data on cybercrime.

[4]While the Department of Defense's Cybercrime Center plays a role in responding to cybercrime and cyber-enabled crime, we did not include the center in our review because its mission related to cybercrime focuses on internal Department of Defense matters.

[5]34 U.S.C. § 41303.

cognizant agency officials regarding differences in how data about cybercrime and other types of crime are collected and reported.

To address our third objective, we reviewed prior GAO work and other relevant reports and literature. We also interviewed cognizant agency officials about any challenges that exist in defining shared metrics for cybercrime and cyber-enabled crime. We analyzed agency responses to identify the number of agencies that reported experiencing the challenge, as well as the factors that contributed to the challenges. Additional details about our objectives, scope, and methodology are in appendix I.

We conducted this performance audit from May 2022 to June 2023 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

As society engages in more personal, business, and governmental activities online, criminals are also shifting their activities online and becoming more sophisticated in exploiting vulnerable populations and threatening public safety and economic security. Cybercrime is a broad term that can refer to a variety of illegal activities that target potential victims online or make use of the internet to carry out illicit activities. Cybercrime can include various types of network intrusions for illicit gain or other malicious purposes, such as ransomware attacks.[6] In addition, traditional criminal activities that are facilitated by the use of the internet—sometimes referred to as "cyber-enabled crime"—can include fraud, identity theft, and the sale of illegal goods.

Cybercrimes can target individuals, private sector companies, critical infrastructure, and government agencies. For example:

- In February 2023, the U.S. Marshals Service reported that it had been the victim of a ransomware attack that impacted a stand-alone computer system containing records about ongoing investigations, employee personal data, and internal processes. The agency reported

[6]Ransomware is a form of malicious software designed to render an individual's or organization's data and systems unusable. Ransom payments are then demanded in exchange for restoring access to the locked data and systems.

that the system did not include personal details about people enrolled in the Federal Witness Protection Program, whose lives could be in danger if publicly exposed. However, the attackers did exfiltrate sensitive files, including information about investigative targets.[7]

- In May 2021, the Colonial Pipeline Company was a victim of a ransomware attack that resulted in a temporary disruption in the delivery of gasoline and other petroleum products across much of the southeastern United States. Specifically, malicious actors reportedly deployed ransomware against the pipeline company's business systems. To ensure the safety of the pipeline, the company proactively disconnected certain systems that monitor and control physical pipeline functions so that they would not be compromised. Disconnecting these systems resulted in a temporary halt to all pipeline operations, though these were subsequently resumed.
- In December of 2020, the cybersecurity firm FireEye discovered that a SolarWinds product known as Orion was compromised and being leveraged by a threat actor for access to SolarWinds' customer systems. According to the SolarWinds Chief Executive Officer, hackers breached the company's network as early as 2019. They inserted malicious code into Orion—a product widely used in both the federal government and private sector to monitor network activity and manage devices. The threat actor, the Foreign Intelligence Service of the Russian Federation, used Orion to breach several federal agency networks. The initial breach opened a backdoor to agency systems that enabled the threat actor to deliver additional malicious code. This allowed them to move laterally, gathering information and compromising data.
- Between 2017 and 2021, the FBI's Internet Crime Complaint Center (IC3) received an average of 552,000 complaints per year. These include complaints of extortion, identity theft, personal data breach, nonpayment or nondelivery, and phishing.[8] In its 2021 annual report, IC3 estimated a total loss of $18.7 billion over this period resulting from these incidents.[9]

[7]Exfiltration is the unauthorized transfer of information from an information system.

[8]Phishing is a technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site in which the perpetrator masquerades as a legitimate business or reputable person.

[9]Federal Bureau of Investigation, *Internet Crime Report 2021*, accessed March 17, 2023, https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf.

- State, local, tribal, and territorial (SLTT) government organizations, including schools, have been particularly targeted by ransomware attacks. These attacks can have devastating impacts on vital government operations and services. According to the Multi-State Information Sharing and Analysis Center—an independent, nonprofit organization—SLTT organizations experienced approximately 2,800 ransomware incidents from January 2017 through March 2021.

Federal Agency Roles and Responsibilities Related to Cybercrime

A number of agencies across the federal government have various roles and responsibilities related to cybercrime, including information gathering, investigation, and prosecution (see table 1).

Table 1: Cybercrime-Related Responsibilities of Selected Agencies

Agency	Responsibilities
Department of Justice (DOJ)	Prosecuting cybercrime via U.S. Attorneys' Offices, Computer Crime and Intellectual Property Section, and—in cases that involve nation-state actors—the National Security Division.
Bureau of Justice Statistics (Statistical agency of DOJ)	Collecting, analyzing, publishing, and disseminating information on crime, criminal offenders, victims of crime, and the operation of justice systems at all levels of government. Providing financial and technical support to state, local, and tribal governments to improve both their statistical capabilities and the quality and utility of their criminal history records. Administering the National Crime Victimization Survey.
Federal Bureau of Investigation (Component of DOJ)	Investigating cyber threats and computer intrusions. Generating, via the Criminal Justice Information Services Uniform Crime Reporting program, statistics for use by law enforcement, including for cyber-related crimes. Collecting and disseminating, via the Internet Crime Complaint Center, reports from the public on suspected internet-facilitated criminal activity.
Bureau of Alcohol, Tobacco, Firearms, and Explosives (Component of DOJ)	Enforcing laws related to the illegal use and trafficking of firearms, the illegal use and storage of explosives, acts of arson and bombings, acts of terrorism, and the illegal diversion of alcohol and tobacco products. This can include investigations of internet-facilitated crimes in these areas.
Drug Enforcement Administration (Component of DOJ)	Enforcing the controlled substances laws and regulations of the United States, including investigating illegal drug trafficking. This can include investigations of internet-related crimes such as the use of the "dark web"[a] or cryptocurrency to facilitate or finance such activities.
U.S. Secret Service (Component of Department of Homeland Security [DHS])	Protecting U.S. financial infrastructure and payment systems by investigating cyber-enabled financial crimes (e.g., wire fraud, credit or debit card fraud, bank fraud, identity theft, and money laundering) and cyberattacks (e.g., intrusions).
Homeland Security Investigations (Component of DHS)	Investigating transnational crime and threats, specifically those criminal organizations that exploit the global infrastructure through which international trade, travel, and finance move. These include cyber-related crimes such as network intrusions, to include exfiltration of export-controlled data and intellectual property, financial fraud, laundering of cryptocurrency, dark web narcotics trafficking and online child sexual exploitation.
Cybersecurity and Infrastructure Security Agency (Component of DHS)	Leading the national effort to understand, manage, and reduce risk to cyber and physical infrastructure. This includes collecting cyber incident reports from critical infrastructure entities and other stakeholders.[b]

Agency	Responsibilities
Internal Revenue Service Criminal Investigation Division (Component of the Department of the Treasury)	Investigating potential criminal violations of the Internal Revenue Code and related financial crimes, including cyber-related violations.
Financial Crimes Enforcement Network (Component of the Department of the Treasury)	Safeguarding the U.S. financial system from illicit use and combating money laundering and its related crimes (including terrorism). Promoting national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence. Collecting Suspicious Activity Reports from financial institutions that identify suspected cases of money laundering or fraud, including those involving cyber events or cyber-enabled crime.
U.S. Postal Inspection Service (Component of the U.S. Postal Service)	Enforcing federal laws covering crimes that include fraudulent use of the U.S. Mail and the postal system, and investigating any crime with a nexus to the mail. These crimes include mail theft, mail fraud, financial fraud, identity theft, robberies and burglaries of postal facilities, assaults and threats on postal employees, investigations of dangerous and prohibited mails, narcotics, and cybercrime.

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

[a]The dark web is a hidden part of the internet that users can access with specialized software to communicate anonymously and engage in illegal activity with little risk of detection.

[b]Critical infrastructure includes the assets, systems, facilities, networks, and other elements that society relies upon to maintain national security, economic vitality, and public health and safety. This includes energy, water systems, commercial facilities, transportation infrastructure, and information and communications networks. In the U.S., this physical and cyber infrastructure is typically owned and operated by the private sector, though some is owned by federal, state, or local governments.

The Better Cybercrime Metrics Act Is Intended to Improve Data and Reporting on Cybercrime

Various organizations and researchers have reported limitations in data about cybercrime and cyber-enabled crime. This includes the underreporting of cybercrime,[10] difficulties obtaining and using digital

[10]Cassandra Dodge and George Burruss, “Policing cybercrime: Responding to the growing problem and considering future solutions,” *The Human Factor of Cybercrime* (Routledge, 2019).

evidence,[11] gaps in the classification of crimes such as cybercrime,[12] and the lack of comprehensive reporting.[13]

The Better Cybercrime Metrics Act, enacted in May 2022, is intended to address deficiencies in the reporting of cybercrime data and establish reporting mechanisms for cybercrime.[14] In passing the law, Congress found that

- public polling indicates that cybercrime could be the most common crime in the United States;
- the United States lacks comprehensive cybercrime data and monitoring, leaving the country less prepared to combat cybercrime that threatens national and economic security; and
- the people of the United States have faced a heightened risk of cybercrime during the COVID–19 pandemic.

The act requires DOJ to, among other things, enter into an agreement with the National Academy of Sciences to develop a taxonomy for categorizing different types of cybercrime and cyber-enabled crime within 90 days of the act's enactment. Also, they are to deliver to Congress a report detailing and summarizing the taxonomy within 1 year of entering into this agreement. In addition, the act requires DOJ, within 2 years of the enactment of the act, to establish a category in the National Incident-Based Reporting System (NIBRS), or any successor system, for the collection of cybercrime and cyber-enabled crime reports from federal,

[11]William A. Carter and Jennifer C. Daskal (authors) and William Crumpler (contributor) "Low-Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge" (Center for Strategic and International Studies: July 2018).

[12]National Academies of Sciences, Engineering, and Medicine, *Modernizing Crime Statistics: Report 1: Defining and Classifying Crime* (Washington, D.C.: The National Academies Press, 2016). https://doi.org/10.17226/23492; National Academies of Sciences, Engineering, and Medicine, *Modernizing Crime Statistics: Report 2: New Systems for Measuring Crime* (Washington, D.C.: The National Academies Press, 2018). https://doi.org/10.17226/25035.

[13]Third Way*, Memo: The Need for Better Metrics on Cybercrime* (Washington, D.C.: Oct. 1, 2019). https://www.thirdway.org/memo/the-need-for-better-metrics-on-cybercrime.

[14]Pub. L. No. 117–116, 136 Stat. 1180 (May 5, 2022).

state, and local officials.[15] Further, it requires DOJ's Bureau of Justice Statistics (BJS) to work with the Department of Commerce's Census Bureau to include questions on cybercrime in the National Crime Victimization Survey within 540 days of the act's enactment.

Prior GAO Reports Related to Cybercrime

We have issued a number of reports on various aspects of cybercrime, such as ransomware, criminal cyber threats to critical infrastructure, and the use of virtual currencies in criminal activity. Table 2 summarizes key findings from selected reports.

Table 2: Selected GAO Reports Addressing Aspects of Cybercrime and Cyber-Enabled Crime

GAO report	Key findings
Global Cybercrime: Federal Agency Efforts to Address International Partners' Capacity to Combat Crime, GAO-23-104768 (Washington, D.C.: Mar. 1, 2023).	A review of federal efforts to build the capacity of allies and partner nations to combat cybercrime. We reported that officials from the Departments of State, Justice (DOJ), and Homeland Security (DHS) and experts from international entities identified six mutual challenges in building global capacity to combat cybercrime. These included a lack of dedicated resources, difficulties in retaining highly trained staff, and inconsistent definitions of "cybercrime." In addition, State, DOJ, and DHS have conducted a variety of activities to build foreign nations' capacity to combat cybercrime. However, State had not conducted a comprehensive evaluation of the agencies' collective efforts. We recommended that State conduct a comprehensive evaluation of capacity building efforts to counter cybercrime, and the department concurred with the recommendation. As of March 2023, the recommendation had not been implemented.
Ransomware: Federal Agencies Provide Useful Assistance but Can Improve Collaboration, GAO-22-104767 (Washington, D.C.: Sept. 14, 2022).	A review of federal efforts to provide ransomware prevention and response assistance to state, local, tribal, and territorial government organizations. We found that the officials from government organizations that we interviewed were generally satisfied with the prevention and response assistance provided by federal agencies. However, they identified challenges related to awareness, outreach, and communication. We made three recommendations to DHS and DOJ to address identified challenges and incorporate key collaboration practices in delivering services to state, local, tribal, and territorial governments. The agencies concurred with our recommendations. As of March 2023, the recommendations had not yet been implemented.
Cyber Insurance: Action Needed to Assess Potential Federal Response to Catastrophic Attacks, GAO-22-104256 (Washington, D.C.: June 21, 2022).	A review of cyber risks to U.S. critical infrastructure, including those posed by criminal groups, and available insurance for these risks. We found that the Department of the Treasury's Federal Insurance Office and the Cybersecurity and Infrastructure Security Agency both had taken steps to understand the financial implications of growing cybersecurity risks. However, they had not assessed the extent to which risks to critical infrastructure from catastrophic cyber incidents and potential financial exposures warrant a federal insurance response. We made two recommendations to the Federal Insurance Office and Cybersecurity and Infrastructure Security Agency to conduct such an assessment and report to Congress on the results. Both agencies concurred with the recommendations. As of March 2023, the recommendations had not yet been implemented.

[15]The National Incident-Based Reporting System (NIBRS) is the system used by the FBI to capture crime data from federal, state, local, tribal, and territorial law enforcement. NIBRS captures details on each single crime incident—as well as on separate offenses within the same incident—including information on victims, known offenders, relationships between victims and offenders, arrestees, and property involved in crimes.

GAO report	Key findings
Virtual Currencies: Additional Information Could Improve Federal Agency Efforts to Counter Human and Drug Trafficking. GAO-22-105462 (Washington, D.C.: Dec. 8, 2021).	A review of the increasing illicit use of virtual currencies to facilitate drug and human trafficking. We found that federal agencies such as the Financial Crimes Enforcement Network (FinCEN) and Internal Revenue Service (IRS) had taken actions to counter the illicit use of virtual currencies but faced challenges. For example, FinCEN and IRS oversee virtual currency kiosks that exchange virtual currencies for cash, but kiosk operators were not required to routinely report the specific locations of their kiosks. We made two recommendations to FinCEN and IRS to review the registration requirements for virtual currency kiosks. Both agencies concurred with the recommendations. As of March 2023, IRS had fully implemented one recommendation, and FinCEN had taken steps to implement the other.
Cybersecurity: Bank and Other Depository Regulators Need Better Data Analytics and Depository Institutions Want More Useable Threat Information, GAO-15-509 (Washington, D.C.: July 2, 2015).	A review of federal oversight and information sharing related to cyber threats, including those posed by criminal groups, to depository institutions such as banks and credit unions. We found that examinations performed by the depository institution regulators generally focused on information technology systems at individual institutions, but most lacked readily available information on deficiencies across the banking system. Further, we found that bank regulators directly address the risks posed to their regulated institutions from third-party technology service providers, but the National Credit Union Administration lacks this authority. We issued a matter for Congressional consideration that Congress modify the Federal Credit Union Act to grant the National Credit Union Administration this authority. As of March 2023, Congress has not granted this authority. We recommended that each of the four regulatory agencies routinely categorize the examination findings and analyze this information to identify trends that can guide areas of review across institutions. The four agencies concurred with the recommendations and have fully implemented them.
Cyberspace: The United States Faces Challenges in Addressing Global Cybersecurity and Governance, GAO-10-606 (Washington, D.C.: July 2, 2010).	A review of significant entities and efforts addressing global cyberspace security and governance issues and challenges to effective U.S. involvement in global cyberspace security and governance efforts. We found that a number of key entities and efforts have significant influence on international cyberspace security and governance, but the global aspects of cyberspace present key challenges to U.S. policy. These challenges included investigating and prosecuting transnational cybercrime amid a plurality of laws, varying technical capabilities, and differing priorities. We made five recommendations to the National Cybersecurity Coordinator to address these challenges. As of March 2023, four of the five recommendation had been implemented. The fifth recommendation—to develop a comprehensive U.S. global cyberspace strategy—was closed as not implemented because the strategy did not establish specific activities, performance metrics, or time frames for achieving results. Such elements are key to assessing how federal efforts support U.S. national security, economic, and other interests.
Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats, GAO-07-705 (Washington, D.C.: June 22, 2007).	A review of the economic and security impacts of cybercrime; the key federal entities, as well as nonfederal and private sector entities, responsible for addressing cybercrime; and challenges in addressing cybercrime. We found that numerous public and private entities have responsibilities to protect against, detect, investigate, and prosecute cybercrime. Further, these entities face a number of challenges in addressing cybercrime, including reporting cybercrime and ensuring that there are adequate analytical capabilities to support law enforcement. We made two recommendations to DOJ and DHS to undertake efforts to help ensure adequate law enforcement analytical and technical capabilities and both recommendations have been implemented.

Source: GAO. | GAO-23-106080

Agencies Use Various Mechanisms to Report Cybercrime and Noted Strengths and Limitations

Agency Reporting Mechanisms Vary by Mission

Agencies use a variety of mechanisms to collect and report data on cybercrime (including cyber-enabled crime). The nature and use of these mechanisms generally depend on the mission and focus of the agencies: identification, investigation, prosecution. Figure 1 summarizes the types of mechanisms used by the agencies in our review for collecting and reporting data on cybercrime.

Figure 1: Types of Mechanisms Agencies in Our Review Used for Reporting Cybercrime

Federal Bureau of Investigation (FBI), Criminal Justice Information Services (CJIS), Cybersecurity and Infrastructure Security Agency (CISA)

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

Identification: Five agencies identify potential or suspected cybercrimes reported by the public or stakeholders and then disseminate that information as appropriate:

- The Bureau of Justice Statistics (BJS) administers the National Crime Victimization Survey, which is the nation's primary source of information on criminal victimization.[16] The survey collects information on nonfatal personal crimes (i.e., rape or sexual assault, robbery, aggravated and simple assault, and personal larceny) and household property crimes (i.e., burglary/trespassing, motor vehicle theft, and other types of theft) both reported and not reported to the police. The survey collects data about specific incidents regarding the location, offender, and type of incident. BJS officials stated that, while the survey collects information on both attempted and threatened crimes, the current definition of "threat" in the survey specifies that it must be delivered verbally and face-to-face; therefore, cybercrimes or crimes committed online do not currently meet the criteria. Though the core National Crime Victimization Survey does not currently collect cybercrime data, BJS has completed some supplemental surveys over the years on various issues that can have a cyber or online component, including stalking, fraud, and identity theft. BJS officials noted that they are in the process of developing categories specific to cybercrime, as required by the Better Cybercrime Metrics Act.
- The Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center (IC3) receives complaints of internet-related crimes from the public and disseminates reports as appropriate to FBI field offices. Complaints are submitted through the Internet Crime Complaint Center Network (IC3Net), an internet-connected FBI network supporting IC3 operations. The main components of IC3Net are a web-based complaint referral form and an associated database of complaint information. The data maintained in the system consist of unclassified information received from the public via the center's online complaint form and additional intelligence information gathered by IC3 personnel. The data also include information about the incident, information about the subject, and personally identifiable information about the complainant and the victim, if different from complainant. Analysts may also search open sources for additional information about a given complaint subject, and when appropriate, may save this open source information within IC3Net. The complaint form does not require the submitter to categorize the incident as a cybercrime; rather, it provides an open text field for a description of

[16]Each year, data are obtained from a nationally representative sample of about 240,000 persons in about 150,000 households. Persons are interviewed on the frequency, characteristics, and consequences of criminal victimization in the United States. The survey does not collect information on crimes against commercial entities.

the incident. Further, IC3 summarizes the data in an annual report to educate on the trends impacting the public.

- FBI's Criminal Justice Information Services' Uniform Crime Reporting program receives reports of crimes from federal and state, local, tribal, and territorial (SLTT) law enforcement agencies via its Uniform Crime Reporting Program and National Incident-Based Reporting System (NIBRS). Specifically, this system receives and collects crime data via automated and manual means from law enforcement at all levels. Federal law enforcement agencies are required to report data to the system, while participation by SLTT agencies is voluntary. NIBRS is intended to collect details on each crime incident as well as on separate offenses within the same incident. These details include information on victims, known offenders, relationships between victims and offenders, arrestees, and property involved in crimes. When law enforcement agencies report incidents to NIBRS, they are required to include a specific code corresponding to the offense (e.g., assault or burglary). As noted previously, the Better Cybercrime Metrics Act required the development of a taxonomy and category for cybercrime to be used in NIBRS or any successor system. While these categories have yet to be developed, the system does include capabilities for identifying incidents that may have a cyber component, such as identity theft. The Uniform Crime Reporting program issues an annual publication on crime in the United States. The program also reports publicly on crime statistics via a publicly accessible website.
- The Cybersecurity and Infrastructure Security Agency (CISA) collects reports of cyber incidents from critical infrastructure entities[17] and other stakeholders, which may include potential cybercrimes.[18] Individuals may report information related to a cybercrime through CISA's incident reporting form. CISA collects these cyber-incident

[17]Critical infrastructure includes the assets, systems, facilities, networks, and other elements that society relies upon to maintain national security, economic vitality, and public health and safety. This includes energy, water systems, commercial facilities, transportation infrastructure, and information and communications networks. In the U.S., this physical and cyber infrastructure is typically owned and operated by the private sector, though some is owned by federal, state, or local governments.

[18]In March 2022, as part of the Consolidated Appropriations Act, 2022, Congress and the President enacted provisions collectively known as the Cyber Incident Reporting for Critical Infrastructure Act of 2022. The law requires CISA to develop and implement regulations requiring covered entities to report covered cyber incidents and ransomware payments to CISA. According to CISA officials, the agency is in the period of developing the Notice of Public Rule Making and determining information requirements. They added that this provides an opportunity to identify metrics that cyber-attack victims must report, which may help clarify the statistics about cyber-attacks and ransomware attacks.

data in a web-based ticketing system. These data sets are populated from incident reports collected through web-based reporting, email reporting, and other telecommunications systems. Incident reports include data such as contact information, information about the organization, a description of the incident, and details on the impact of the incident. The reported cyber incidents are coded based on the type of incident, and these codes may align with certain cybercrimes (e.g. denial-of-service attacks, like ransomware). CISA officials noted that they do not report on cybercrime; however, they do refer instances of suspected cybercrime to the FBI.

- The Financial Crimes Enforcement Network (FinCEN) is responsible for maintaining information provided by financial institutions pursuant to the Bank Secrecy Act (BSA). FinCEN collects Suspicious Activity Reports from financial institutions when they identify suspected cases of illicit financial activity, which can include cases with a cyber-component. This includes filings of suspicious financial activity possibly related to cyber-enabled crime, which are collected in the agency's BSA reporting database. Details specific to cyber-related activities that are collected may include information about the location of the victim, a date-stamped internet protocol address associated with a fraudulent login, an email domain used by an attacker, or cryptocurrency payment addresses used in a ransomware attack. This information is stored in FinCEN's reporting database, and information can be entered into specific data fields using established codes. Information may also be entered in narrative fields. FinCEN shares the reports it receives with interagency partners.

Investigation: Investigative agencies such as the FBI; the Drug Enforcement Administration (DEA); Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF); Secret Service; Immigration and Custom Enforcement's Homeland Security Investigations (HSI); IRS's Criminal Investigation Division; and the U.S. Postal Inspection Service use electronic case management systems to collect data on criminal investigations, including those with a cyber component.

- FBI Field Offices collect cybercrime data using the agency's Sentinel case management system. This system includes investigative, intelligence, personnel, and administrative data collected by the FBI in the course of conducting its mission. The system assigns each case a numeric code based on the category of the investigation. This includes codes designating a case by the type of threat program, such as counterterrorism or computer intrusions. When agents open an investigation, they are required to assign specific tags to the case, which provides more specificity to the cases. These include tags for

cybercrime threats or money laundering. The tags also allow them to pull the number of cases being worked on a specific topic. Each field office can run reports based on case codes and threat tags. In addition, officials stated that reports are often conducted at the headquarters level. They added that field offices may review aggregate data to determine whether open cases matches staffing levels.

- The Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF) collects cybercrime data using its N-Force case management system. N-Force is a computer-based case management system that supports ATF's law enforcement operations by providing automated collection, dissemination, management, and analysis of investigative data. For each case, N-Force captures and reports on categories of data, including people involved, events, property, and locations. The N-Force system has a checkbox feature that allows investigators to indicate if an investigation includes certain cyber-related aspects such as "cryptocurrency," "internet search," and "social media exploitation." According to ATF officials, the collection of such data is driven by the agency's field investigations. ATF officials further reported that the agency's case management system tracks cyber-related aspects of investigations and these data could be retrieved. However, the agency does not perform trend analysis or reporting on these data.
- The Drug Enforcement Administration (DEA) tracks investigative data using its Investigative Management Program and Case Tracking System, which may include cybercrime data. This web-based case management system supports the establishment, recording, accessibility, and analysis of information pertaining to DEA investigative activities. According to DEA officials, the agency's investigative system does not have a specific field for characterizing an investigation as cybercrime. However, investigators can enter text in the system to indicate an internet-related aspect. In addition, field investigators can request assistance from the agency's Cyber Support Section when an investigation involves a cyber aspect (e.g., the use of cryptocurrency or a need for cyber forensics). Because requests for cyber-related support are made on a case-by-case basis, DEA officials stated that they do not formally report data on these cases. However, DEA's Chief Data Officer stated that the agency wants to start tracking these cyber-related cases more centrally.
- U.S. Secret Service collects cybercrime data using its Field Investigative Reporting System (FIRS), which provides the framework for a suite of software applications used by the agency. Each FIRS application offers tools that help users find, gather, analyze, and share

data related to the investigative missions of the Secret Service. The Incident-Based Reporting application allows agents to view and enter case data for Secret Service criminal investigations. In this application, Secret Service tracks 11 primary case types, six of which are designated as cyber. The primary case types correspond to violations of the U.S. Code for which the Secret Service has authority. For example, "Unauthorized Access to Network or Computer" is a case type that corresponds to the violation of 18 U.S. Code § 1030, the Computer Fraud and Abuse Act. Agency officials reported that their Enterprise Analytics Division produces automated dashboards, updated monthly with open and closed cyber financial cases as well as "the Amount of Cyber Financial Loss Prevented," an official DHS performance metric. This division also produces various reports on closed cyber financial cases that are reviewed on a monthly and quarterly basis for validation and verification purposes.

- The Internal Revenue Service's (IRS) Criminal Investigation Division collects and tracks data using its Criminal Investigations Management Information System, which includes all opened cases at the agency, including cyber related. Agents enter the information into the system, which requires inputting information into mandatory fields such as the type of case, fraud indicators, scheme codes, and applicable program area. To track cybercrime, the system uses a series of special purpose codes. These codes are typically entered manually by the special agents in the field working on cyber and cyber-related investigations. These data points are then incorporated into reports. For example, if there is a cyber-related case with a fraud scheme code for virtual currency, that case will be included in cyber reporting. IRS officials explained the Criminal Investigation Division has an annual report that breaks down annual statistics, such as the number of cases being worked or cases prosecuted. This report includes details on cybercrime efforts and digital forensics, among other things.
- The United States Postal Inspection Service (USPIS) uses its Case Management System, which is an integrated, online database that assists in documenting and tracking criminal investigations, including cyber cases. The system classifies crimes by attributes, some of which are used to identify cybercrime. Additionally, it can also calculate the number of cases by attributes, such as the number of "dark web"-related cases.[19] USPIS can perform key word searches to identify which crimes had a nexus related to social media and crypto currency. According to USPIS officials, there are no system-generated

[19]The dark web is a hidden part of the Internet that specialized software enables users to access with little risk of detection.

or automated reports on cybercrime. However, the Case Management system provides an "on demand" report where all cyber categorized cases can be listed.

- Immigration and Customs Enforcement's Homeland Security Investigations (HSI) uses its Investigative Case Management System to document its investigations. The system allows for multiple modes of data entry relating to cyber related crime. Users can enter in reports of investigation, which allow for free-text input of investigative actions. In addition, users can select from drop-down fields for specific report types such as "victim identification," "search warrant executed on internet service provider/digital/electronic media," and "computer forensics information." These report types have specific drop downs to assist users with inputting relevant data. The system also has a number of other different user forms, such as to document the search of a cell phone or tablet device, and to document the search of electronic devices such as computers. In addition, the system contains unique project codes to identify cybercrime-related investigations or reports such as network intrusion operations, child exploitation, and financial fraud. These project codes are searchable and contribute to tracking of metrics but rely on case agents and local managers to appropriately enter them. All data in the system are contained in an HSI-owned data warehouse that can be queried by the Data Management and Reporting Unit. In addition, the Cyber Crimes Center tracks cyber-related investigations and queries its systems periodically to identify cyber-dependent and cyber-enabled crimes.[20] For example, at the start of a new fiscal year, HSI queries its systems to determine the number of cyber-enabled and cyber-dependent cases that were investigated in the previous fiscal year.

Prosecution: DOJ (through U.S. Attorney's Offices and other DOJ components) prosecutes crimes, including cybercrime, which are tracked using case management systems. For example:

- The Computer Crime and Intellectual Property Section (CCIPS) is a specialized prosecution office responsible for prosecuting crimes related to computer intrusions and providing legal and technical

[20]According to DHS, HSI's Cyber Crimes Center provides investigative and technical field support, subject matter expertise, training, and other services in support of cybercrime investigations.

support to other offices that manage cyber-related cases.[21] CCIPS tracks its cases using a case management system known as Docket, which includes cases categorized as computer intrusions. According to officials, 90 percent of CCIPS cases are cyber-related, and these are tracked according to the law under which the case is charged, such as the Computer Fraud and Abuse Act.[22] While the system does not identify "cybercrime" as such, CCIPS officials noted that any case charged under the Computer Fraud and Abuse Act could be considered an instance of cybercrime. Officials added that they report aggregate statistics of the cases to the DOJ Criminal Division Front Office.

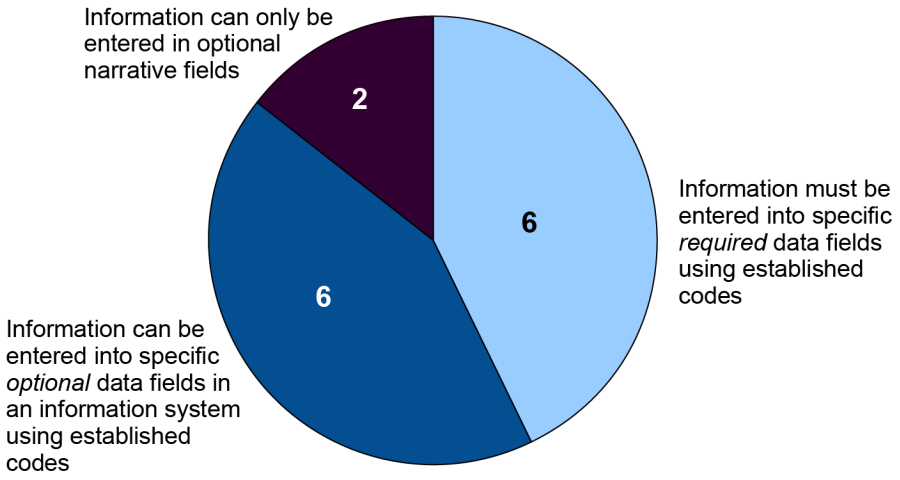
- The National Security Division (NSD) investigates and prosecutes computer intrusions and attacks by nation-state actors, terrorists, and their proxies, as well as those that target the military or the intelligence community. NSD tracks what it considers "cyber matters" in its case management system. According to NSD officials, this system, the Litigation Case Management System, has functionality for identifying cases as "cyber related" and can generate reports based on this information.

Agencies have various types of functionality in their information systems for collecting data on cybercrime and cyber-enabled crime. These types of functionality include (1) required data fields using established codes to categorize cybercrime and/or cyber-enabled crime, (2) optional data fields used to categorize these crimes, and (3) narrative fields where information on cyber-aspects of crime can be entered. Figure 2 shows the number of agency systems with each type of functionality.

[21]For example, the Computer Crime and Intellectual Property Section (CCIPS) provides specialized litigation support to the 93 United States Attorneys in cases involving cybercrime or cyber-enabled crimes. CCIPS officials also noted that the U.S Attorneys use a system called CaseView, which is managed by the Department of Justice's (DOJ) Executive Office for U.S. Attorneys, to track their cases.

[22]The Computer Fraud and Abuse Act, codified at 18 U.S.C. § 1030, creates several crimes and civil causes of action, such as prohibiting access without authorization to certain computers, including ones used in or affecting interstate or foreign commerce.

Figure 2: Functionality That Selected Agency Systems Used to Collect Cybercrime-Related Data



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

Agencies Identified Strengths and Limitations in Mechanisms for Reporting Cybercrime and Cyber-Enabled Crime

Agencies identified several strengths and limitations in the mechanisms used to collect and report data on cybercrime and cyber-enabled crime. Strengths included system functionality for capturing attributes of and classifying cybercrime or cyber-enabled crime, as well as various information-sharing activities. Limitations included the lack of a common definition of cybercrime or cyber-enabled crime, the variations in how and to what extent agencies collect these data, and the absence of a central repository for cybercrime data.

Strengths of Existing Reporting Mechanisms

Agencies reported a number of strengths associated with the mechanisms they use for reporting cybercrime and cyber-enabled crime. These include:

- **Systems with specific functionality for capturing cybercrime data enable case and investigation tracking.** As described above, some agency systems, such as case management systems, include functionality for categorizing crimes as cybercrimes (including cyber-enabled crimes). They may also tag crimes as relying on a particular technique, such as ransomware. The degree of automation for this functionality varies, with some agencies classifying cybercrimes using a system of codes, some systems including a drop-down menu or a checkbox for indicating crimes with cyber components, and other

systems having fields for entering text to describe an investigation or incident as cyber related. For example, one agency assigns codes to cases in its case management system, including codes for cases identified as cybercrime or cyber-enabled crime. Another agency's case management system includes drop-down tags that allow cases to be identified as cyber related. A third agency uses text fields to indicate cyber aspects to a case (e.g., the technique used) and tracks such cases using a collaboration software site to provide investigative support to field agents.

- **Agency systems may include capabilities for querying reports on cybercrime**. Specifically, some agencies have the capability to query their systems to generate reports of cybercrimes or crimes that relied on a particular technique. For example, one agency noted that it can run reports based on case codes, which include codes for cybercrime, cyber enabled-crime, and terrorism. They also assign threat tags to cases that allow the agencies to pull the number of cases being worked on a specific topic, such as the number of opened cases related to money laundering or cyber intrusion. Another agency pulls reports based on defined attributes of crime, which can include cybercrimes or cyber-enabled crimes.
- **Agency systems facilitate collaboration and information sharing**. In particular, agencies noted that their systems allow them to share information pertaining to specific cases as part of an ongoing investigation. For example:
  - Nine agencies (Secret Service, CISA, HSI, FBI, ATF, DEA, CCIPS, USPIS, and IRS) reported sharing information from their case management systems on cybercrimes, though this is often on a case-by-case basis, depending on the particular investigation. This includes sharing data as may be required to cooperate on a case or to support analysis, such as in the annual Verizon Data Breach Investigations Report. In addition, FinCEN distributes information on cybercrime or cyber-enabled crime to its agency partners.
  - Three agencies (CJIS, IC3, and BJS) are responsible for creating public reports on crimes in the United States, which may include cyber or internet crime. These reports draw on data collected via their various systems. For example, IC3's annual Internet Crime Report includes details on the number of complaints, reported financial losses, most commonly reported crime types, and where crimes occurred.

- In addition, five agencies (Secret Service, CISA, HSI, USPIS, and IRS), described participating in task forces that focus on information sharing and investigative support on specific cybercrime concerns such as ransomware. For example, CISA co-chairs the Joint Ransomware Task Force with the FBI. The task force provides a framework to support interagency coordination on counter ransomware initiatives. Such efforts draw on information collected in agencies' systems while carrying out their respective missions.

Limitations of Existing Mechanisms

Agencies reported a number of limitations associated with the mechanisms they use for reporting cybercrime and cyber-enabled crime. These include:

- **Agencies lack a common definition of cybercrime**. Specifically, agencies noted that there is no single agreed-upon definition of cybercrime or cyber-enabled crime across the government or among law enforcement agencies. Agencies varied in the extent to which they formally defined this for themselves, with some agencies noting that it is not a major focus of their mission. For example, one agency noted that it generally uses the term "cybercrime" to refer to criminal activity committed using a computer but does not independently define cybercrime or cyber-enabled crime. Another agency specified that it prefers to use the term "computer intrusions." Accordingly, even to the extent that they are tracking similar crime data in their systems, agencies may not be identifying the same types of offenses as "cybercrime" or "cyber-enabled crime."
- **Agency systems vary in the manner and extent to which they collect data on cybercrime, which limits their ability to consistently track data**. For example, not all agencies' systems have specific functionality for capturing cybercrime data, such as codes, categories, and tags that can be applied to each relevant case. Some systems rely on text fields and agent discretion. Since several systems do not have categories for capturing different types of cybercrime, they may rely on narrower categories, such as identity theft. For instance one agency's reporting system includes categories for two types of crimes potentially related to cybercrime—identify theft and hacking—but not cybercrime as such. Another agency uses a case management system to track all crimes it is investigating, but the system is limited to using an open text field to indicate a crime with a cyber-component. Accordingly, agencies may not be capturing these data in a uniform manner or to the same extent.

- **Data on cybercrime are not collected at a centralized location**. Agencies collect cybercrime data that pertain to their own ongoing investigations, but these data are not currently collected in a centralized location. For example, FBI's IC3 receives complaints from the public and refers them to law enforcement, but this only provides a partial picture of the total amount of reported cybercrime (i.e., incidents reported by members of the public, but not by law enforcement or other sources).

  Similarly, FBI's NIBRS is to collect reports on crime from federal and SLTT law enforcement. However, as noted previously, NIBRS currently has limited categories for capturing data on cybercrime and cyber-enabled crime. While the Better Cybercrime Metrics Act calls for the establishment in NIBRS of a category for the collection of cybercrime and cyber-enabled crime data, FBI officials noted that a challenge in implementing this requirement is the time it will take to coordinate with the criminal justice community regarding the appropriate data points to capture cybercrime incidents.

Provisions of the Better Cybercrime Metrics Act are aimed at addressing some of the existing limitations in how cybercrime data are collected and reported. In particular, the development of a cybercrime taxonomy and category in FBI's NIBRS system target the lack of a common definition and uniform approach to collecting data on cybercrime. The taxonomy is due to be completed one year after DOJ enters into its agreement with the National Academies of Science, and the establishment of a cybercrime category is due to be completed in May 2024. Thus, while it is too early to tell how effective these efforts will be in addressing existing limitations, we plan to monitor these activities.

Agencies Noted Differences between Reporting Cybercrime and Other Crimes

As we have reported, cybercrime differs from traditional crimes primarily in the techniques that are used.[23] In particular, cybercrime techniques have characteristics that can vastly enhance the reach and impact of criminal activity. For example:

- Criminals do not need to be physically close to their victims to commit a crime.
- Technology allows criminal actions to easily cross state and national borders.

[23]GAO-07-705.

- Cybercrime can be carried out automatically, at high speed, and by attacking a vast number of victims at the same time.
- Cybercriminals can more easily remain anonymous.

The selected agencies identified several differences between how they collect or report data on cybercrime (including cyber-enabled crime) and other types of crime, including how cybercrime is categorized and underreported.

Cybercrime is not consistently tracked or identified. Agencies do not necessarily track cybercrime (including cyber-enabled crime) separately from other types of crime. According to several agencies, this is because they generally track crimes based on the violation that occurred. By contrast, cybercrimes are distinguished by the technique used and may fall under several different violations (e.g., computer intrusion, theft, or fraud). For example, one agency noted that its reporting does not distinguish between cybercrime and other types of crime. Instead, personnel report on their investigative activities by assigned case types, which are the primary criminal charge being pursued. Another agency noted that it uses the same mechanism for reporting cybercrimes and other crimes and does not distinguish between them. A third agency stated that it does not indicate in its case tracking system whether the case is cyber related, but each case includes the statutes the crime is being charged under.

Agencies added that they only identify cybercrimes as such when there is a specific mission need to do so. For example, one agency noted that while it does not systematically report cybercrime data, crimes are flagged as cyber related when there is a particular element identified by a field agent. In other cases, agencies only note this when an investigation requires specialized technical support, such as digital forensics or familiarity with virtual currencies. Further, one agency noted that it has no overarching policy or mandate to collect this type of data. Additionally, as discussed previously, agency systems vary in the functionality they have to collect and track data on cybercrime. Further, the way agencies collect and track such data is generally driven by their missions. For example, one agency noted that its system is focused on collecting traditional crime data, though the system allows for placing crimes into certain potentially cyber-related categories (e.g., identity theft committed via the internet or hacking).

Cybercrime is likely underreported. Both GAO and others have reported that cybercrime is likely underreported.[24] When a cybercrime is detected, entities and individuals can choose to report it to law enforcement or not. They weigh the cost and impact of the incident with the time and effort needed to support an investigation and prosecution. In addition, our work and that of the Congressional Research Service related to information sharing have shown that businesses do not always want to report being the victim of a cybercrime because there is a perception that this information will be disclosed publicly, which could, in turn, cause harm to their business. Further, victims of cybercrime or cyber-enabled crime may not be knowledgeable about cybercrime, and one agency noted that there is no one standard way for the public to report.

Several of the selected agencies also noted the underreporting of cybercrime and cyber-enabled crime. For example, one agency noted that often victims do not know what government entity to report cybercrime to, or they may lack the ability to provide the entire picture of the crime or differentiate between the various types of cybercrimes. Another agency stated that, if it is not entirely clear who can do anything about it, victims lack an incentive to report cybercrime. In addition, victims are likely more accustomed to reporting crime to local authorities rather than federal agencies. Moreover, businesses or other entities may be reluctant to report cybercrime because of concerns about reputational impact. Another agency noted that it relies on field agents to report crimes with a cyber component, but this only occurs when the agent needs specialized investigative support from headquarters. Further, those reporting may not be familiar with or able to accurately collect technical information related to the crime.

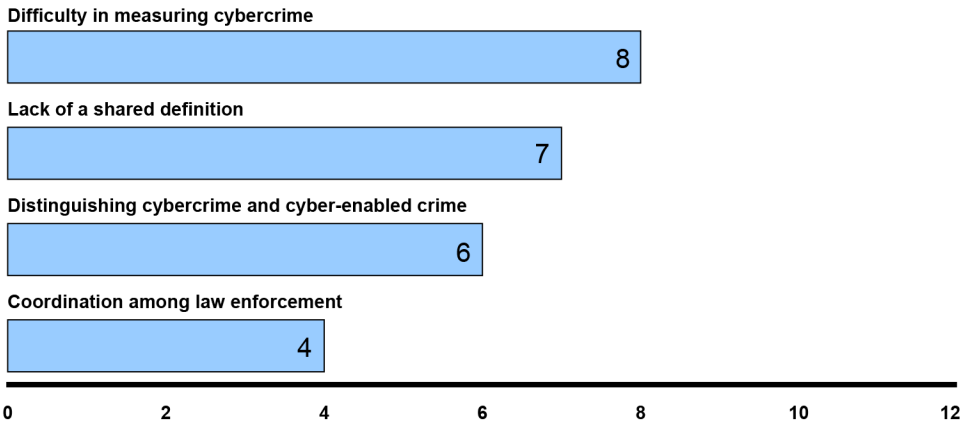
Agencies Identified Challenges in Establishing Cybercrime Metrics

Most of the agencies selected for our review reported challenges in developing a shared set of metrics for measuring cybercrime, including cyber-enabled crime. The challenges cited by most agencies were difficulty in measuring the extent or impact of such crime and the lack of a shared definition. Additionally, agencies and components cited challenges related to distinguishing between cybercrime and cyber-enabled crime, and challenges with coordination among law enforcement agencies

[24]See, for example, GAO-07-705 and Congressional Research Service, *The Economic Impact of Cyber Attacks*, RL 32331 (Washington, D.C.: Apr. 1, 2004).

pertaining to cybercrime events. Figure 3 shows the challenges and the number of selected agencies that cited them.

Figure 3: Challenges in Establishing Cybercrime Metrics



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

Difficulty in measuring the extent or impact of cybercrime: Specifically, eight of the 12 agencies (HSI, FBI, DEA, BJS, NSD, CCIPS, FinCEN, and IRS) reported that developing metrics to measure the extent or impact of cybercrime was inherently difficult. In addition to the difficulty in measuring cybercrime, agencies also cited challenges in defining metrics to measure the impact of countermeasures and the avoidance of cybercrime. For example:

- IRS officials noted that it had existing standards for tracking data components such as the number of criminal prosecutions and seizures. However, those traditional metrics did not capture the scope of cybercrime or the impact of the efforts, such as the number of cyberattacks prevented, the amount of personally identifiable information that did not end up in the hands of criminals, or the amount of sensitive information retrieved from the dark web.
- CCIPS officials noted that because of the scale and breadth of cybercrime, it is hard to determine the quantity or quality of its impact. For example, they noted that credit card fraud may inconvenience someone, but generally, credit card companies may restore the victim's financial loss. However, cyberstalking or phishing can have a much larger impact, such as people losing their life savings.

Additionally, CCIPS officials stated that it was hard to talk with the victims of cybercrime. For example, in the case of many "traditional" crimes, prosecutors would talk to victims to better understand the impact. However, in the case of a cybercrime that could affect thousands or even millions of people, this is not practical.

- IRS officials reported that cybercrime often has downstream effects that are not widely known or clear at the time of the investigation. For instance, a hacker may steal personal information that is then sold on the dark web. The stolen information may then be used for a host of frauds including romantic, identity, tax, credit card, or benefit fraud. However, these crimes are not always committed by the same group and not always timed near each other. Thus, the effects can last years and take a significant amount of effort by individuals and agencies to resolve. Further, the agency reported that it was also challenged to identify the collateral impacts outside of traditional metrics such as loss of revenue and stolen funds.

Lack of a shared definition: Seven of 12 agencies (HSI, FBI, DEA, BJS, CCIPS, USPIS, and IRS) reported that the lack of a shared definition of cybercrime impedes the development of shared metrics. Specifically, given the lack of a standardized definition and varying definitions used by law enforcement agencies, significant work would be required to collect consistent and comparable data on cybercrime. For example:

- FBI officials noted that there is no specific uniform classification across entities, and it is difficult to come up with a classification that fits everything. The officials added that one can have a broad classification like phishing, but to have more details would require additional subcategories. Thus, trying to merge everything is a challenge.
- CCIPS officials stated that a lot of crime could be considered cybercrime or cyber-enabled crime by the public. However, these crimes would not necessarily be charged under the current Computer Fraud and Abuse Act because that statute does not encompass every action that could be considered cybercrime or cyber-enabled crime. As a result, they focus on the specific elements and charges for a case. They may describe a case as a "cybercrime" or "cyber-enabled" informally or in press statements, but there is no clear universal definition of "cybercrime" or "cyber-enabled crime." Also, criminal conduct and technology both continue to evolve. Additionally, the agency acknowledged that "cybercrime" is not a legally precise term and that an agreed-upon definition would help to talk about the problems and various programs for counting and reporting. For

example, nation-states may commit acts that could be considered cybercrimes—such as theft of data or damage to computer systems—if done by an individual or group, but the national security community may consider these acts of espionage or sabotage because of the actor involved.

- BJS officials reported that they were reviewing various proposed definitions and an initial review found differing definitions across federal, state, and local law enforcement agencies. Officials noted the importance of getting a resolution on these definitional issues because of the extent of victimization and the different ways that cybercrime is manifested.

Distinguishing between cybercrime and cyber-enabled crime: Six of 12 agencies (HSI, FBI, DEA, BJS, CCIPS, and USPIS) reported a challenge in distinguishing between cybercrime and cyber-enabled crime for the purposes of developing metrics. Specifically, agencies noted that the boundaries between cybercrime and cyber-enabled crime were not always clear and that they had to rely on ad hoc distinctions between these types of crime. For example:

- DEA officials stated that they would consider a crime an instance of cybercrime when individuals attack the cyber infrastructure with a variety of goals and methods. By contrast, cyber-enabled crime, would involve the use of cyber tools to conduct traditional criminal activity.
- CCIPS officials said that it tended to describe “cybercrime” as offenses affecting the confidentiality, availability, or integrity of computer systems, such as computer intrusions, damage, or taking unauthorized control of a system. “Cyber-enabled crimes” tended to be crimes made possible or easier by computers or the internet (e.g., online fraud or illicit online marketplaces).
- Two agencies (HSI and IRS) noted that they used a different term—”cyber-dependent crime.” IRS defined this as crimes that would not exist without the internet (e.g., hacking, ransomware and remote access). HSI reported using the term to periodically query its database for statistical reporting.
- FBI officials stated that the lack of distinction was a challenge and added that the inability to distinguish between cybercrime and cyber-enabled crime hinders efforts to study, measure, or categorize these types of specific crimes.

Coordination among law enforcement agencies: Four of 12 agencies (HSI, FBI, BJS, and CCIPS) stated that coordinating among federal and

SLTT law enforcement agencies is a challenge in developing shared cybercrime metrics. Specifically, developing comparable data on cybercrime across law enforcement would require agencies to agree on matters such as definitions and which types of data to collect. For example:

- BJS officials reported that the definition of cybercrime is at the heart of the coordination issues. This is due, in part, to the criteria of what rises to the level of a crime for an online threat varying from one state's law enforcement groups to another.
- FBI officials reported that entities classify things differently, and there is no specifically uniform classification. If a broad classification is defined, it will need to be granular and allow subcategories to capture details.
- In addition, FBI officials noted that establishing the cybercrime category in NIBRS will require extensive coordination with the criminal justice community. According to FBI, as of April 2023, 13,390 agencies were submitting data via NIBRS. These agencies represent 70 percent of the total agencies submitting data, covering 76.5 percent of the population. However, according to FBI officials, fewer than half of federal law enforcement agencies report to NIBRS, and participation by SLTT agencies is voluntary and getting all agencies to participate continues to be a challenge.

Finally, five agencies noted additional challenges related to developing metrics for cybercrime:

- FBI officials stated that challenges impeding the transition to NIBRS reporting include a lack of available funding, insufficient training of personnel who need to use the system, and concerns that the switch to NIBRS reporting will contribute to a public perception that crime has significantly increased. FBI officials also described efforts they have made to assist agencies in switching to NIBRS, such as technical support and no-cost training. They added that they will continue these and similar efforts, as well as engaging field staff and outside partners to convey the importance of using NIBRS to the law enforcement community.
- FinCEN officials stated that reports by financial institutions may reveal only certain facets of cybercrime activity. Additionally, this agency stated that there are gaps in reporting from international partners that share information.

- CCIPS officials reported the government often lacks reporting or details about cybercrime because victim reporting is not mandatory except for certain relatively narrow categories of cybercrime victims. Incident response firms in the private sector often have better information and metrics about the events and scope of attacks on their clients because they are often the first group brought in after an intrusion or damage is discovered.
- HSI officials cited challenges including continuous engagement and training of its field offices and investigators related to cybercrime. This included listing appropriate program codes or areas in its case management system.
- DEA officials noted that there are limited resources and uniform collection of this type of data across the U.S. government.

The provisions of the Better Cybercrime Metrics Act, such as those that require the development of a cybercrime taxonomy and reporting categories, if effectively implemented, should help address these challenges. As previously noted, DOJ was to enter into an agreement with the National Academies to develop the taxonomy within 90 days from the enactment of the act, with the report on the details of the taxonomy to Congress due 1 year after that. In addition, the establishment of a cybercrime category in NIBRS or its successor system is due to be completed in May 2024.

In April 2023, DOJ officials told us that they had not yet entered into the agreement with the National Academies to develop the cybercrime taxonomy but had created two documents supporting the development of the agreement. They added that these documents are currently pending the approval of the Attorney General. The first is a document that would delegate authority to the FBI to engage with the National Academies on behalf of the Attorney General. The second is a statement of work for the taxonomy project as required by the act. They added that FBI officials are maintaining contact with all collaborators to ensure project readiness once a signed delegation of authority letter is received. The officials did not state how much of a delay, if any, this would have in developing the taxonomy.

Agency Comments

We provided a draft of this report to the agencies in our review for review and comment. IRS stated that it had no comments. The remaining agencies provided technical comments, which we incorporated as appropriate.

We are sending copies of this report to the appropriate congressional committees, the heads of the agencies in our review, and other interested parties. In addition, the report is available at no charge on the GAO website at https://www.gao.gov.

If you or your staff have any questions about this report, please contact Marisol Cruz Cain at (202) 512-5017or cruzcainm@gao.gov or Gretta Goodwin at (202) 512-8777 or goodwing@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix II.

Marisol Cruz Cain, Director
Information Technology and Cybersecurity

Gretta L. Goodwin, Director
Homeland Security and Justice

Appendix I: Objectives, Scope, and Methodology

The objectives of this review were to identify (1) the existing mechanisms used to report cybercrime and cyber-enabled crime in the United States and the strengths and limitations that have been reported in these mechanisms, (2) the differences between data reported on cybercrime or cyber-enabled crime and other types of crime, and (3) the challenges selected agencies reported in defining shared metrics for tracking cybercrime and cyber-enabled crime in the United States.

We focused this review on selected federal agencies with responsibilities related to cybercrime. We identified key agencies with responsibilities for identifying, investigating, and prosecuting cybercrime based on a review of previous GAO work in this area[1] and by consulting internal GAO stakeholders with subject matter expertise. We also solicited input from agencies we spoke with identify additional agencies or offices that play a role in collecting data related to cybercrime. Based on this process, we selected the following agencies and offices:[2]

Department of Homeland Security

- United States Secret Service
- Cybersecurity and Infrastructure Security Agency
- Immigration and Customs Enforcement's Homeland Security Investigations

Department of Justice

- Federal Bureau of Investigation (including its Baltimore field office,[3] Criminal Justice Information Services Division, and Internet Crime Complaint Center)
- Drug Enforcement Administration

[1]See, for example, GAO, *Virtual Currencies: Additional Information Could Improve Federal Agency Efforts to Counter Human and Drug Trafficking*, GAO-22-105462 (Washington, D.C.: Dec. 8, 2021); *Cyberspace: The United States Faces Challenges in Addressing Global Cybersecurity and Governance*, GAO-10-606 (Washington, D.C.: July 2, 2010); and *Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats*, GAO-07-705 (Washington, D.C.: June 22, 2007).

[2]While the Department of Defense's Cybercrime Center plays a role in responded to cybercrime and cyber-enabled crime, we did not include the center in our review because its cybercrime-related mission focuses on internal Department of Defense matters.

[3]We met with the FBI's Baltimore Field Office to understand how FBI field personnel may collect and report data on cybercrime.

- Bureau of Alcohol, Tobacco, Firearms, and Explosives
- Computer Crime and Intellectual Property Section
- National Security Division
- Bureau of Justice Statistics

Department of the Treasury

- Internal Revenue Service-Criminal Investigation
- Financial Crimes Enforcement Network

U.S. Postal Service

- U.S. Postal Inspection Service

To identify the existing mechanisms used to report cybercrime and cyber enabled crime, we reviewed relevant federal laws, including the Better Cybercrime Metrics Act and the Uniform Federal Crime Reporting Act of 1988.[4] In addition, we reviewed agency policies, procedures, and other documentation on processes for collecting, maintaining, sharing, and reporting data on cybercrime and cyber-enabled crime, including any agency definitions. We also reviewed documentation on the systems (e.g. databases, case management systems) used by agencies to collect, share, and report data on cybercrime and cyber-enabled crime. We identified functionality included in agencies' information systems to categorize and report on cybercrime and cyber-enabled crime. Lastly, we interviewed cognizant agency officials about their processes and mechanisms for collecting and reporting data on cybercrime and cyber-enabled crime, including the strengths and limitations in existing reporting mechanisms.

To identify the differences between data reported on cybercrime or cyber-enabled crime and other types of crime, we reviewed agency policies, procedures, and documentation. Further, we reviewed relevant GAO reports and other literature. We also interviewed cognizant agency officials, asking them to identify any such differences.

To identify the challenges selected agencies reported in defining shared metrics for tracking cybercrime and cyber-enabled crime in the United States, we reviewed prior GAO work and other relevant reports and literature. We then interviewed cognizant agency officials about any

[4]34 U.S.C. § 41303.

challenges that exist in defining shared metrics for cybercrime and cyber-enabled crime. After compiling a list of potentially common challenges, we gathered written input from all the agencies about whether they had experienced those challenges and what factors contributed to those challenges. We analyzed agency responses to identify the number of agencies that reported experiencing the challenge, as well as the factors that contributed to the challenges.

We conducted this performance audit from May 2022 to June 2023 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: GAO Contacts and Staff Acknowledgments

GAO Contacts

Marisol Cruz Cain, (202) 512-5017, cruzcainm@gao.gov

Gretta L. Goodwin, (202) 512-8777, goodwing@gao.gov

Staff Acknowledgments

In addition to the contacts listed above, the following staff made key contributions to this report: Rosanna Guerrero and Joseph P. Cruz (assistant directors), Lee McCracken (analyst in charge), Amanda Andrade, Lauri Barnes, Kiana Beshir, Michelle Bird, Christopher Businsky, Andrew Stavisky, Julia Vieweg, Adam Vodraska, and Marshall Williams, Jr.