Congressional
Research Service
Informing the legislative debate since 1914

# Justice Department's Role in Cyber Incident Response

Updated December 18, 2020

Congressional Research Service
https://crsreports.congress.gov
R44926

CRS REPORT
Prepared for Members and
Committees of Congress

# Summary

Criminals and other malicious actors rely on the Internet and evolving technology to further their operations. In cyberspace, criminals can compromise financial assets, hacktivists can flood websites with traffic—effectively shutting them down, and spies can steal intellectual property and government secrets. When such cyber incidents occur, a number of questions arise, including how the federal government will react and which agencies will respond.

Presidential Policy Directive/PPD-41 outlined how the government responds to significant cyber incidents. Responding to these incidents involves (1) threat response, (2) asset response, and (3) intelligence support. The Department of Justice (DOJ), through the Federal Bureau of Investigation (FBI, or the bureau) and National Cyber Investigative Joint Task Force (NCIJTF), is the designated lead on threat response, which involves investigating and attributing specific cyber activities to particular individuals or entities as well as facilitating intelligence and information sharing.

In investigating cyber incidents, the FBI's cyber priorities are focused on "high-level intrusions by state-sponsored hackers, global organized crime syndicates, and other technically sophisticated and dangerous actors." In addition to conducting its own cyber investigations, the FBI

- leads the NCIJTF, a multiagency hub for coordinating, integrating, and sharing information on cyber threat investigations;
- heads up other task forces and law enforcement partnerships focused on cyber threat response, including cyber task forces with subject matter experts at each field office, cyber action teams that can rapidly deploy in response to specific incidents, and cyber assistant legal attachés positioned in certain foreign countries to work with U.S. counterparts;
- established initiatives to interface with the private sector regarding cyber incidents; these resources (such as the Internet Crime Complaint Center, InfraGard program, and National Cyber-Forensics and Training Alliance) collect and share information, build partnerships, and enhance cyber threat awareness;
- has worked to recruit and retain an appropriate cyber workforce and has developed a multilayered cyber training program for its agents; and
- has discussed with the technology community and policymakers how evolving technology, such as encrypted communications and devices, affects investigations, particularly in cyber-related cases, and how law enforcement can develop tools to investigate these cases most effectively.

Relating to the FBI's work in combating and responding to cyber threats, one question policymakers may have is how the bureau *prioritizes* cyber threats. DOJ's Inspector General, while noting strides in this arena, has recommended that (1) the FBI should use a more data-driven, objective methodology to identify and prioritize cyber threats, and (2) the FBI should develop a means to track agent time spent on specific cyber threats. Policymakers may elect to conduct oversight of the FBI's efforts in these areas, examine whether any changes to cyber threat prioritization affect where cyber threats rank within the broader universe of threats confronting the nation, and debate whether or how to direct the FBI's use of funds allocated to combating cyber threats.

# Contents

## Contacts

Criminals and other malicious actors rely on the Internet and evolving technology to further their operations.[1] They exploit cyberspace, where they can mask their identities and motivations. In this domain, criminals can compromise financial assets, hacktivists can flood websites with traffic—effectively shutting them down, and spies can steal intellectual property and government secrets.

When such cyber incidents occur, a number of questions arise, including how the federal government will react and which agencies will respond. These questions have been raised following a number of high-profile breaches such as those against the U.S. Office of Personnel Management[2] and the Democratic National Committee,[3] as well as intrusions into a number of federal agencies and other organizations via network management software produced by SolarWinds.[4] Federal law enforcement has taken the lead in investigating cyber incidents, attributing certain malicious activities to specific perpetrators, and prosecuting cyber threat actors.

This report outlines the federal framework for cyber incident response, highlighting the Department of Justice's (DOJ's) role in this response. It also discusses challenges for federal law enforcement and potential policy issues for Congress.

# Defining a Cyber Incident

A principal issue in understanding how the federal government *responds* to a cyber incident is the definition of a "cyber incident." A host of terms are used in discussing malicious activity with a cyber, online, or technological component. These range from cyber attack and cyberwarfare to cybercrime, cyber espionage, and cyber terrorism. A key distinction between these malicious incidents is the actor's motivation. For instance, a criminal may be profit motivated, while a terrorist may be politically motivated. However, "[t]he speed and anonymity of cyber attacks makes distinguishing among the actions of terrorists, criminals, and nation states difficult, a task which often occurs only after the fact, if at all."[5]

"Cyber incident," therefore, is an umbrella term encompassing a range of malicious activity carried out by diverse actors with varying motivations and capabilities—all of whom exploit cyberspace.[6] The federal government has defined a cyber incident as

[1] For more information on cybercrime, see CRS Report R42547, *Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement*.

[2] For information on the OPM breach, see archived CRS Report R44111, *Cyber Intrusion into U.S. Office of Personnel Management: In Brief*.

[3] For more information on the hack of the Democratic National Committee, see Wired, *DNC-HACK*, https://www.wired.com/tag/dnc-hack/.

[4] For more information on intrusions via software produced by SolarWinds, see Krebs on Security, *Malicious Domain in SolarWinds Hack Turned into 'Killswitch'*, December 16, 2020.

[5] Department of Homeland Security, *National Strategy to Secure Cyberspace*, February 2003, p. viii.

[6] The National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23) defines cyberspace as "the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries." In other words, cyberspace is the "virtual environment of information and interactions between people." National Security Agency, *Statement for the Record, Lieutenant General Keith Alexander, Commander, Joint Functional Component Command for Network Warfare*, Before the House Armed Services Committee, Terrorism, Unconventional Threats, and Capabilities Subcommittee, May 5, 2009.

> [a]n event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon.[7]

As such, an incident could capture an array of activities carried out by malicious actors ranging from hacktivists and criminals to nation states and terrorists. Notably, the federal government has not developed official definitions for specific subsets of cyber incidents—such as cybercrime—that distinguish them from other subsets of cyber incidents.[8]

# U.S. Cyber Incident Response

Federal law enforcement has the principal role in investigating and attributing cyber incidents to specific perpetrators, and this responsibility has been established within the broader framework of federal cyber incident response.[9] The 2016 Presidential Policy Directive/PPD-41 outlined how the government responds to *significant* cyber incidents—those that are "likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people."[10] Responding to cyber incidents involves (1) threat response, (2) asset response, and (3) intelligence support. DOJ, through the Federal Bureau of Investigation (FBI) and National Cyber Investigative Joint Task Force (NCIJTF), is the designated lead on *threat response*.[11] Asset response and intelligence support responsibilities are led by other federal agencies.[12]

The concept of threat response, as outlined by PPD-41, involves

> conducting appropriate law enforcement and national security investigative activity at the affected entity's site; collecting evidence and gathering intelligence; providing attribution; linking related incidents; identifying additional affected entities; identifying threat pursuit and disruption opportunities; developing and executing courses of action to mitigate the

[7] The White House, *Presidential Policy Directive—United States Cyber Incident Coordination*, PPD-41, July 26, 2016. The PPD noted that this definition could include vulnerabilities in information systems, system security procedures, internal controls, or implementation that could ultimately be exploited by a threat actor.

[8] For a policy discussion on potential benefits of cyber incident definitions (such as a definition of cybercrime), see CRS Report R42547, *Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement*.

[9] The White House, "Fact Sheet: Presidential Policy Directive on United States Cyber Incident Coordination," press release, July 26, 2016.

[10] The White House, *Presidential Policy Directive—United States Cyber Incident Coordination*, PPD-41, July 26, 2016.

[11] For more information on the FBI's cyber investigations, see https://www.fbi.gov/investigate/cyber/. Information on the NCIJTF is available at https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force.

[12] The Department of Homeland Security, through the National Cybersecurity and Communications Integration Center, is the lead on asset response. The Office of the Director of National Intelligence, through the Cyber Threat Intelligence Integration Center, is the lead on intelligence support. Asset response activities include, among other things, "technical assistance to affected entities to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents; identifying other entities that may be at risk and assessing their risk to the same or similar vulnerabilities; [and] assessing potential risks to the sector or region ... and developing courses of action to mitigate these risks." Intelligence support activities "facilitate the building of situational threat awareness and sharing of related intelligence; the integrated analysis of threat trends and events; the identification of knowledge gaps; and the ability to degrade or mitigate adversary threat capabilities." See The White House, *Presidential Policy Directive—United States Cyber Incident Coordination*, PPD-41, July 26, 2016.

> immediate threat; and facilitating information sharing and operational coordination with asset response.[13]

Due to the nature of crime and other malicious activity in the technology era, a number of departments and agencies with law enforcement capabilities are involved in responding to cyber threats.[14] This section, however, highlights the activities led by DOJ—specifically, by the FBI.

## FBI Cyber Investigations

The FBI pursues cybercrime cases ranging from computer hacking and intellectual property rights violations to child exploitation, fraud, and identity theft. Its top priorities involve combating computer and network intrusions and investigating ransomware. While some of these cases may be significant cyber incidents, others may not. The FBI's cyber priorities are focused on "high-level intrusions by state-sponsored hackers, global organized crime syndicates, and other technically sophisticated and dangerous actors."[15] One key challenge, acknowledged by officials and others, is how to move away from reacting to malicious cyber events and toward preventing them.[16]

Indeed, the multifaceted approach of the FBI's new cyber strategy involves not only responding to cyber incidents through arrest and indictments but also working with a range of public and private partners to share information about cyber threats to prevent and react to incidents.[17] The hub of these partnerships within the federal government is the NCIJTF, led by the FBI. In addition, the FBI established the National Defense Cyber Alliance to share intelligence with the defense industry and the National Cyber-Forensics and Training Alliance to share information with industry partners, academia, and the financial sector. The FBI also runs a number of cyber task forces and has been working to enhance its cyber workforce.

### National Cyber Investigative Joint Task Force

The NCIJTF was established by National Security Presidential Directive-54/Homeland Security Presidential Directive-23 in January 2008. As established, the NCIJTF's mission is to "serve as a multi-agency national focal point for coordinating, integrating, and sharing pertinent information related to cyber threat investigations."[18] The NCIJTF coordinates the efforts of more than 30 U.S. agencies including law enforcement, intelligence, and the military. It also collaborates with the private sector and international partners.

[13] The White House, *Presidential Policy Directive—United States Cyber Incident Coordination*, PPD-41, July 26, 2016.

[14] Notably, not all cyber incidents will be investigated by law enforcement. For instance, some intrusions on a private network may be evaluated by internal investigators or other private companies. Other cyber incidents may just be deemed nuisances and not investigated at all.

[15] Statement of FBI Director Christopher Wray before the U.S. Congress, Senate Homeland Security and Governmental Affairs Committee, *Worldwide Threats*, 116th Cong., 1st sess., November 5, 2019.

[16] Statement of former FBI Director James B. Comey before the U.S. Congress, House Committee on the Judiciary, *Oversight of the Federal Bureau of Investigation*, 114th Cong., 2nd sess., September 28, 2016.

[17] Federal Bureau of Investigation, "CISA Cybersecurity Summit: Addressing Threats Through Partnerships," press release, September 16, 2020; Jory Heckman, "FBI cyber strategy maximizes deterrence through agency partnerships," *Federal News Network*, October 1, 2020.

[18] The White House, *National Security Presidential Directive-54/Homeland Security Presidential Directive-23*, January 8, 2008. See also https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force.

One major initiative of the NCIJTF, Operation Clean Slate, aims to disrupt and dismantle significant botnets threatening the United States.[19] In one prominent case under Operation Clean Slate, the FBI led an international law enforcement effort to disrupt the GameOver Zeus botnet.[20] GameOver Zeus was a variant of the Zeus botnet, which would steal online banking information and transfer funds to money mules, U.S. residents with bank accounts who would move the money out of the United States. In this case, law enforcement was authorized to sever communication between infected computers and criminal-controlled servers. Officials also indicted an alleged administrator of GameOver Zeus, "charging him with conspiracy, computer hacking, wire fraud, bank fraud, and money laundering."[21]

Early in its inception, there were concerns about the effectiveness of the NCIJTF. One was that "the NCIJTF was not always sharing information about cyber threats among the partner agencies."[22] There were also criticisms that the NCIJTF was perceived as an extension of the FBI's Cyber Division rather than as a multiagency effort—potentially hindering its collaborative mission. DOJ's Inspector General noted in 2015 that these issues had improved.[23]

In combining resources of the NCIJTF with its own, the FBI runs a 24-hour cyber command center known as CyWatch. This center is charged with "coordinating domestic law enforcement response to criminal and national security cyber intrusions, tracking victim notification, and partnering with other federal cyber centers."[24]

## Cyber-Related Task Forces and Partnerships

The FBI leads a variety of law enforcement task forces and partnerships focused on cyber threat response.

- There is a Cyber Task Force (CTF) at each field office. These CTFs focus on local cybersecurity threats, respond to incidents, and maintain relationships with companies and institutions. They also support the national effort to combat cybercrime by participating in national virtual teams on certain cyber issues and providing cyber subject matter experts or surge capability outside of their territories, when needed.[25]
- In 2006, the FBI established Cyber Action Teams (CATs) of agents and computer scientists that can be rapidly deployed around the country or the world to assist in

[19] A botnet refers to a collection of computers that have been compromised by malicious code and are controlled across a network. See Cybersecurity and Infrastructure Security Agency, *Cybersecurity Glossary*, https://niccs.cisa.gov/about-niccs/cybersecurity-glossary.

[20] Testimony by Robert Anderson, Jr., Federal Bureau of Investigation, before the U.S. Congress, Senate Committee on Homeland Security and Governmental Affairs, *Cybersecurity, Terrorism, and Beyond: Addressing Evolving Threats to the Homeland*, 113th Cong., 2nd sess., September 10, 2014.

[21] U.S. Department of Justice, "U.S. Leads Multi-National Action Against GameOver Zeus Botnet and Cryptolocker Ransomware, Charges Botnet Administrator," press release, June 2, 2014.

[22] Department of Justice, Office of the Inspector General, *The Federal Bureau of Investigation's Ability to Address the National Security Cyber Intrusion Threat*, April 2011.

[23] Department of Justice, Office of the Inspector General, *Audit of the Federal Bureau of Investigation's Implementation of Its Next Generation Cyber Initiative*, July 2015.

[24] Department of Justice, *Report of the Attorney General's Cyber Digital Task Force*, July 2, 2018, p. 90.

[25] Federal Bureau of Investigation, *Cyber Task Forces: Building Alliances to Improve the Nation's Cybersecurity*.

computer-intrusion investigations. CAT members have expertise in various computer languages, forensic investigations, and analysis of malware.[26]

- In addition to domestic field offices pursuing international leads in investigations, the FBI has positioned cyber assistant legal attachés (ALATs) in some foreign countries. These ALATs work with law enforcement in host countries to share information, collaborate on investigations, and enhance relationships with partner agencies. They focus on "identifying, disrupting, and dismantling cyber threat actors and organizations."[27]

## Private Sector Information Sharing and Collaboration

In addition to its partnerships with law enforcement, the FBI has established several initiatives to interface with the private sector regarding cyber incidents. They collect and share information, build partnerships, and enhance awareness.

- The FBI stood up the Internet Crime Complaint Center (IC3) in 2000. Its mission is two-fold: (1) act as a reporting mechanism for the public to submit information on potential criminal activity facilitated by the Internet, and (2) foster law enforcement and industry alliances. Information is shared with law enforcement to bolster investigative and intelligence activities and with the public to enhance awareness.[28] Law enforcement can remotely search the IC3 database through the FBI's Law Enforcement Enterprise Portal.[29]
- InfraGard is a collaboration between the FBI and private sector partners. These partners include business executives, entrepreneurs, computer professionals, academia, the military, law enforcement, and other government officials. The program facilitates information sharing with the goal of protecting U.S. critical infrastructure.[30] The alliance originally focused on cyber threats and has since expanded to include other threats that might impact critical infrastructure.
- The National Cyber-Forensics and Training Alliance (NCFTA) is a nonprofit information-sharing organization bringing together subject matter experts from law enforcement, the private sector, and academia to target cybercrime.[31] The NCFTA produces unclassified intelligence assessments and develops strategies to

[26] Federal Bureau of Investigation, *The Cyber Action Team: Rapidly Responding to Major Computer Intrusions*, March 4, 2015.

[27] Federal Bureau of Investigation, *National Cyber Security Awareness Month: FBI Deploys Cyber Experts to Work Directly With Foreign Partners*, October 26, 2016. ALATs have been placed in locations including London, England; The Hague, Netherlands; Tallinn, Estonia; Kyiv, Ukraine; and Ottawa, Canada, among others. See also Frank Cilluffo and Val Cofield, "Why the FBI's cyber attachés are so valuable," *CyberScoop*, June 24, 2020.

[28] Federal Bureau of Investigation, Internet Crime Complaint Center, *2019 Internet Crime Report*, February 2020.

[29] For more information on this portal, see https://www.fbi.gov/services/cjis/leep.

[30] For more information on InfraGard, see https://www.infragard.org/. The critical infrastructure sectors are chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services and banking, food and agriculture, government facilities, healthcare and public health, information technology, transportation systems, water and wastewater treatment systems, and nuclear reactors, materials, and waste. See Cybersecurity and Infrastructure Security Agency, *Critical Infrastructure Sectors*, https://www.cisa.gov/critical-infrastructure-sectors.

[31] For more information on the NCFTA, see https://www.ncfta.net/.

> mitigate cyber threats. The FBI can use this information to initiate or bolster law enforcement investigations.[32]

While mechanisms have been developed to share information between the FBI and the private sector, a number of barriers to effective sharing have been highlighted. These include "(1) a perception by the private sector that information flows in one direction—to the FBI; (2) information, when provided by the FBI, is often not useful because it lacks context or is outdated; and (3) private sector concerns regarding how the FBI will use the information that is shared."[33] With respect to the concern about unidirectional information flow, some of the information becomes part of ongoing investigations and is thus marked as law enforcement sensitive or otherwise classified, which limits its sharing. However, the FBI has developed unclassified products that it can share with private sector partners that include information on technical indicators and information private entities can use to bolster protection for their networks as well as contextual information on current threats posed by cyber criminals.[34] Some private sector entities have noted that the information they receive from the FBI can be outdated or lacking substance. When the FBI receives information on cyber threats, it may take time to scrub sensitive or classified information from reports that it can share with its private sector partners. In a similar vein, private entities may be reluctant to share information with the FBI out of concerns surrounding how the FBI may handle—or potentially release—proprietary information and personally identifiable information from companies' records.[35] The FBI has noted that, even after a breach, a majority of private sector partners do not automatically engage federal investigators and instead turn to private firms for attribution and remediation.[36] For instance, the Democratic National Committee retained a firm named CrowdStrike to secure its network when it discovered a breach—attributed to the Russian government.[37] The FBI has been encouraging private companies and organizations to reach out directly to law enforcement to help investigate, attribute, and mitigate breaches.

Of note, the FBI indicated that many victims of cyber breaches—often companies and organizations—do not know they have suffered an intrusion until the FBI notifies them.[38] The bureau had established Cyber Guardian "for tracking the production, dissemination, and disposition of cyber victim notifications which can help victims mitigate the damage caused by cyber intrusions and increase the potential for intelligence collection by the FBI." DOJ's Inspector General found the data in Cyber Guardian to be incomplete and unreliable, thus preventing the FBI from knowing whether all victims had been notified of breaches.[39] The FBI

[32] Department of Justice, Office of the Inspector General, *Audit of the Federal Bureau of Investigation's Implementation of Its Next Generation Cyber Initiative*, July 2015.

[33] Ibid., p. 19.

[34] Ibid.

[35] Ibid.

[36] Federal Bureau of Investigation, *The FBI and Cyber Crime: New Perspectives, New Partnerships, and New Ways of Doing Business*, March 29, 2017.

[37] Ellen Nakashima, "Russian Government Hackers Penetrated DNC, Stole Opposition Research on Trump," *The Washington Post*, June 14, 2016. For more information on the attribution, see Schneier on Security, *Attributing the DNC Hacks to Russia*, January 9, 2017; as well as Laura Hautala, "How US Cybersleuths Decided Russia Hacked the DNC," *CNet*, May 3, 2017.

[38] Department of Justice, Office of the Inspector General, *Audit of the Federal Bureau of Investigation's Cyber Victim Notification Process*, March 2019.

[39] Ibid.

has been in the process of replacing Cyber Guardian with a system called CyNERGY; assessments of this system have not been made public.

Congress has, for some time, shown an interest in cyber information sharing; in the context of examining the FBI's response to cyber threats, policymakers may specifically look into information sharing between the private sector and federal law enforcement. They may debate whether Congress can or should help reduce barriers to information sharing. While some have noted potential benefits of increased information sharing, there have also been concerns that such sharing—specifically in the direction of public to private—could potentially compromise law enforcement investigations and national security.[40]

## Cyber Workforce

In addressing the cyber threat, the FBI faces challenges in both recruiting and retaining an appropriate cyber workforce.[41] On the recruitment side, former FBI Director James Comey noted that it can be challenging to find agents with integrity, fitness, intelligence, *and* specialized cyber knowledge. One solution might be rethinking whether there should be multiple classes of agents recruited to work on cyber cases. For instance, some of these individuals might have specialized knowledge but do not need to carry a firearm. Another option that has been floated involves easing the current requirement that agents who leave the FBI and wish to return after two years or more must go through the FBI's training academy again.[42] Policymakers may consider how such changes to the hiring structure could impact the FBI's budgetary resources needed for hiring, training, and retaining cyber-focused agents.

On the retention side, DOJ's Inspector General recommended that the FBI, among other things, "evaluate the effectiveness of the step-by-step training course for FBI agents on how to investigate national security intrusion cases; reconsider the rotation policy for cyber agents and ensure that agents skilled and experienced in cyber intrusions are available to FBI field offices; and consider developing regional hubs with agents that are experts in investigating national security intrusions."[43] The FBI has evolved its strategy on assigning computer-intrusion cases. These cases are now assigned to the field office that has demonstrated the greatest strength in investigating a particular type of intrusion, rather than to the field office in the area where the intrusion occurred.[44] The bureau has noted this fosters competition between field offices to bolster agents' knowledge and skills.

The FBI has a multifaceted cyber training program for agents, and this training has been revised based on results of an internal survey the bureau conducted on it.[45] FBI cyber training includes (1) a High Technology Environment Training initiative to bolster the technical skills and

[40] For more information on the broad issue of cyber information sharing, see CRS Report R43941, *Cybersecurity and Information Sharing: Legal Challenges and Solutions* (available to congressional clients upon request).

[41] Federal Bureau of Investigation, *The FBI and Cyber Crime: New Perspectives, New Partnerships, and New Ways of Doing Business*, March 29, 2017.

[42] Ibid.

[43] Department of Justice, Office of the Inspector General, *Audit of the Federal Bureau of Investigation's Implementation of Its Next Generation Cyber Initiative*, July 2015, p. ii.

[44] Federal Bureau of Investigation, *The FBI and Cyber Crime: New Perspectives, New Partnerships, and New Ways of Doing Business*, March 29, 2017.

[45] Department of Justice, Office of the Inspector General, *Audit of the Federal Bureau of Investigation's Implementation of Its Next Generation Cyber Initiative*, July 2015.

technological knowledge of the full FBI workforce, (2) SANS Institute[46] training courses for cyber personnel, and (3) opportunities for certain personnel to earn a Master of Science degree in information technology.[47]

## Technology and Investigations

FBI investigators seek to use every tool in their cyber investigative toolkit to combat a range of threats and attribute activities to specific threat actors. Law enforcement has expressed concern that investigators' capabilities may be outpaced by the speed of technological change. For instance, factors influencing law enforcement's ability to obtain information include strong, end-to-end encryption; provider limits on data retention; bounds on companies' technological capabilities to produce specific data points for law enforcement; tools facilitating anonymity online; and a landscape of mixed wireless, cellular, and other networks through which individuals and information are constantly passing.[48] Much of the discourse in this area is around whether law enforcement should have "lawful access" to information that may be secured by end-to-end, or what investigators have called "warrant proof," encryption.[49] Notably, law enforcement supports strong encryption to protect networks, devices, and information. However, they note that malicious actors also exploit the widespread use of strongly encrypted communications and devices. Experts have generally recommended that the FBI deploy resources to strengthen its investigative competencies—rather than asking technology companies to build exploitable weaknesses or "backdoors" into their products—so that it can best respond to cyber and other threats.[50]

Lawmakers and officials have continued to discuss how best to simultaneously protect the privacy of encrypted devices and communications as well as support legitimate law enforcement access. In 2016, for instance, members of the House Judiciary Committee and Energy and Commerce Committee established an Encryption Working Group to "identify potential solutions that preserve the benefits of strong encryption—including the protection of Americans' privacy and information security—while also ensuring law enforcement has the tools needed to keep us safe and prevent crime."[51] Four points from the working group's year-end report may contribute to policy discussions in Congress: (1) any measure that weakens encryption would work against the nation's security interests, (2) encryption technology is widely used and increasingly available worldwide, (3) there is no one-size-fits-all solution to the encryption and going dark challenge,

[46] The SANS Institute is a private entity that offers cyber security and information security training.

[47] Department of Justice, Office of the Inspector General, *Audit of the Federal Bureau of Investigation's Cyber Threat Prioritization*, July 2016.

[48] For more information on evolving technology and law enforcement investigations, see CRS Report R44481, *Encryption and the "Going Dark" Debate*.

[49] Law enforcement describes warrant-proof encryption as that where only the end user has access and thus may hinder a lawful court order or search warrant. See Federal Bureau of Investigation, *The Lawful Access Challenge*, https://www.fbi.gov/about/leadership-and-structure/science-and-technology-branch/lawful-access; See also Andrea Peterson, "The Government and Privacy Advocates Can't Agree on What 'Strong' Encryption Even Means," *The Washington Post*, October 7, 2015; Herb Lin, "The Rhetoric of the Encryption Debate," *Lawfare*, October 12, 2015.

[50] See, for example, testimony by Susan Landau before U.S. Congress, House Committee on the Judiciary, *The Encryption Tightrope: Balancing Americans' Security and Privacy*, 114th Cong., 2nd sess., March 1, 2016.

[51] House Judiciary Committee, "Goodlatte, Conyers, Upton, and Pallone Announce Bipartisan Encryption Working Group," press release, March 21, 2016.

and (4) Congress should promote cooperation between the law enforcement and technology communities.[52]

## FBI Cyber Threat Prioritization

Relating to the FBI's work in combating and responding to cyber threats, one question policymakers may have is how the bureau *prioritizes* cyber threats. The FBI conducts an annual Threat Review and Prioritization (TRP) to delineate the top threats—cyber and other—and direct resource allocation. Within the broader threat prioritization framework, DOJ's Inspector General looked specifically at the FBI's prioritization of cyber threats from FY2014-FY2016.[53] The Inspector General's report made two recommendations:

- The FBI should use an "algorithmic, data-driven, and objective methodology" to identify and prioritize cyber threats.[54] This recommendation is based on the Inspector General's findings that the TRP criteria are subjective and open to interpretation. Changing the methodology may give the FBI a better view of the threat landscape and help the bureau accurately prioritize threats.
- The FBI should "[d]evelop and implement a record keeping system that tracks agent time utilization by threat."[55] The bureau currently tracks agent time by case classification (such as public corruption or counterterrorism), not specific threats. As such, it may not be able to evaluate resources dedicated to any given threat and evaluate whether a specific cyber threat has been appropriately prioritized.

The FBI concurred with both recommendations. It has reportedly been bolstering its Cyber Division's Threat Examination and Scoping (TExAS) tool, which relies on specific data and a weighted algorithm rather than subjective rankings to prioritize cyber threats. The bureau is also reportedly looking into potential changes to its record-keeping system to track agent time utilization.[56] Congress may elect to exercise its oversight to examine whether (and if so, how) the FBI has made any adjustments to its cyber threat prioritization regimen. They may also question whether any changes to this regimen could affect where cyber threats fall within the broader framework of threats facing the nation. This could, in turn, have implications for how Congress directs the FBI to use its appropriated funds.

[52] House Judiciary Committee and House Energy and Commerce Committee, Encryption Working Group, *Encryption Working Group Year-End Report*, December 20, 2016.

[53] Department of Justice, Office of the Inspector General, *Audit of the Federal Bureau of Investigation's Cyber Threat Prioritization*, July 2016.

[54] Ibid., p. 17.

[55] Ibid.

[56] Ibid., p. 22. The FBI does not appear to have released any more detailed information on its cyber threat prioritization tool.

## Author Information

Kristin Finklea
Specialist in Domestic Security

## Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.