THIRD WAY

Reader's Guide to Understanding the US Cyber Enforcement Architecture and Budget

by Brandon Gaskew

Takeaways

The United States is facing a rising cybercrime wave, affecting every sector of the US economy and threatening America's national security. Despite this growing threat, there is a serious gap in the US government's response—our research has found that less than 1% of malicious cyber incidents ever see an arrest of the criminal. This cyber enforcement gap has allowed cybercriminals to operate with impunity and must be addressed in congressional responses to the issue.

Many US government entities have the responsibility of reducing the cyber enforcement gap and Congress must assess whether they have the necessary resources to shrink the gap. To help in these efforts during the Fiscal Year (FY) 2020 budget cycle, Third Way has prepared a Reader's Guide for Members of Congress and their staff to help them understand the key government entities involved in cyber enforcement and their current funding levels.

While much of the budget levels for key cyber enforcement entities in the US government have remained either flat or, in certain cases, been increased, this has little impact on the cyber enforcement gap. Congress should provide additional resources to make more progress in reducing the cyber enforcement gap.

This Reader's Guide includes three sections:

1. An introduction to the US cyber enforcement gap and a proposal to reduce the gap by rebalancing US cybersecurity policy from a heavy focus on network security to a policy that also goes after the human attacker using law enforcement and diplomacy;
2. A mapping of the key federal government departments and agencies with a role in cyber enforcement; and
3. An overview of current budget levels for cyber enforcement across key government entities where information is publicly available.

The United States is facing a rising cybercrime wave, yet, a tremendous enforcement gap currently exists in government efforts to identify, stop, and punish the human cyber attackers.

The United States and countries around the globe are currently facing a stunning gap in their efforts to bring to justice cybercriminals and other malicious cyber actors. This national security and economic threat continues to rise, while offensive efforts to counter it have fallen short.

A rising and often unseen cybercrime wave is mushrooming in America. There are approximately 300,000 reported malicious cyber incidents reported to the Federal Bureau of Investigation per year hitting every sector of the US economy— which is likely a vast undercount since many victims do not report break-ins to begin with.[1] Malicious cyber activity perpetrated by nation-states, criminal networks, terrorist groups, lone actors, and others has cost the US economy anywhere from $57 billion to $109 billion annually and these costs are increasing. Cybercrime tools have been used to attack vital US national security institutions and steal critical information. A single one of these incidents can hit countless victims in many different countries no matter the location of the perpetrators.[2]

Third Way has launched a new Cyber Enforcement Initiative aimed at identifying policy solutions to boost the governments' ability to identify, stop, and punish malicious cyber actors.[3] Through this Initiative, Third Way has found that, on average, only 3 out of 1,000 of the malicious cyber incidents that occur in the United States annually see an arrest, which is an enforcement rate of less than 1%.[4] This cyber enforcement gap is allowing criminals to engage in malicious behavior without any fear of being caught or punished.

Government is the only institution with the authority to pursue the human attacker and bring them to justice. However, in the United States, a heavy focus of cyber policy discussions has been building better cyber defenses against intrusion. To close the cyber enforcement gap, Third Way has argued we must rebalance US cyber policy from a predominant emphasis on network protection to a policy that also uses law enforcement to go after the human cyber attackers and diplomacy to boost international cooperation and capacity in order to do so.

In order to rebalance America's cyber approach and prioritize law enforcement and diplomacy, the country needs a comprehensive strategy for strengthening the US government's abilities to identify, stop, and punish cybercriminals and other malicious cyber actors. To help develop such a strategy, Congress must start by first understanding the key government entities involved in cyber enforcement and assess whether their current funding levels meet the challenges they are faced with in reducing the cyber enforcement gap.

There are a multitude of government entities involved in cyber enforcement and Congress must assess whether they have the needed resources to make progress in reducing the cyber enforcement gap.

There are eight federal departments that have a key role in cyber enforcement. These entities have a role in cybercrime prosecutions, investigations, international cooperation efforts, and international law enforcement capacity building. Yet, the resources provided to these government entities have not been sufficient to stem the growing cyber enforcement gap. As such, Congress should assess the current levels of resources and authorities involved in cyber enforcement to ensure they are aligned to reduce the cyber enforcement gap.

There are eight federal departments and several law enforcement agencies involved in cyber enforcement. This includes the Department of Justice, which is the main US law enforcement agency that leads much of the government's work to prosecute cybercrime through its Criminal Division, National Security Division, and Office of the United States Attorneys. The Department of Justice also has cybercrime investigation functions through its law enforcement agencies such as the FBI. The Department of Homeland Security has an active role in cybercrime investigations as a result of overseeing the United States Secret Service and US Immigration and Customs Enforcement's Homeland Security Investigations. Further, the Department of Treasury oversees several offices with a role in investigating financial crimes as well as administering US cyber-related sanctions. On the international front, the Department of State, programs at the Department of Justice, and the United States Agency for International Development work to build the capacity of global criminal justice systems to investigate and prosecute cybercrimes and boost international cooperation in these efforts. State and local law enforcement agencies also lead on many cybercrime investigations.

With the expanding list of entities involved in cyber enforcement, issues such as mission duplication, misallocation of resources, and unclear lines of authority have arisen. While each of these agencies has a vital role in cyber enforcement, there are also some similar or overlapping responsibilities between them. At the federal level in particular, this can lead to inefficiencies, redundancies, and difficulties in ensuring congressional oversight efforts are tied to an overarching strategic cyber enforcement approach across agencies.[5]

To help make sense of all of the different government entities involved in cyber enforcement, Third Way has prepared a Reader's Guide for Members of Congress and their staff. This document is meant to give a snapshot of the key entities involved in making progress in reducing the cyber enforcement gap. This list is not exhaustive, and some government agencies were not included if they do not have a predominant focus on cyber enforcement.[6] The list of Departments, Agencies, Offices, Sections, and Divisions were selected because of their key role in either cybercrime prosecutions, investigations, international cooperation, or international capacity building.

The following agencies play a critical role in US cyber enforcement efforts:

THIRD WAY

LEGEND

- ATF: Bureau of Alcohol, Tobacco, Firearms and Explosives
- CRM: Criminal Division
- FBI: Federal Bureau of Investigation
- INTERPOL Washington
- ICE: U.S. Immigrations and Customs Enforcement
- INL: Bureau of International Narcotics and Law Enforcement
- IRS: Internal Revenue Services
- NCCIC: National Cybersecurity and Communications Integration Center
- NSD: National Security Division
- S/CCI: Office of the Coordinator for Cyber Issues
- SLTT: State, Local, Tribal, and Territorial (SLTT) Law Enforcement Agencies
- TFI: Office of Terrorism and Financial Intelligence
- USAO: United States Attorney's Offices
- USMS: U.S. Marshals Service

This list of federal departments and agencies is not exhaustive. It is a compilation of key government entities with a core mission in cyber enforcement. There are many other federal entities who work in this area.

1. Currently, the Office of the Cyber Coordinator for Cyber Issues has been folded into the Division of International Communications and Information within the Bureau of Economic and Business Affairs. There is Congressional legislation to establish an Office of International Cyberspace Policy at the State Department, with the office reporting to the undersecretary of state for political affairs.

Department of Justice (DOJ)

Criminal Division (CRM)

Computer Crime and Intellectual Property Section (CCIPS)

- CCIPS investigates and prosecutes computer crimes and works to prevent the theft of intellectual property (i.e. copyright, trademark, or trade-secrets).[7]

Organized Crime and Gang Section (OCGS)

- OCGS investigates and prosecutes transnational organized crime groups with a cyber nexus.[8]

Money Laundering and Asset Recovery Section (MLARS)

- MLARS leads DOJ's asset forfeiture and anti-money laundering enforcement efforts and prosecutes international cybercrime cases involving financial institutions.[9]

Office of International Affairs (OIA)

- OIA leads DOJ in its international cooperation efforts in cybercrime investigations through five main areas: (1) extradition and removal of cybercriminals; (2) transfer of sentenced cybercriminals; (3) international cybercrime evidence gathering between countries; (4) providing legal advice to DOJ leadership and prosecutors; and (5) international relations and treaty matters.[10]

Office of Overseas Prosecutorial Development Assistance and Training (OPDAT)

- OPDAT works to target transnational cybercriminal organizations and leads an international prosecutorial capacity-building mission, which works with partner governments to improve responses to computer crime and strengthen cybersecurity.[11]

International Criminal Investigative Training Assistance Program (ICITAP)

- ICITAP works with foreign governments to build the capacity of their law enforcement institutions on a wide range of issues, including cybercrime investigations.[12]

National Security Division (NSD)

National Security Cyber Specialists (NSCS)

- NSCS is a network of nearly 100 prosecutors located in US Attorney's Offices nationwide and cyber experts from NSD and CCIPS who can be deployed to provide expertise in cyber investigations.[13]

Counterintelligence and Export Control Section (CES)

- CES prosecutes and investigates threats involving cyber-based espionage and state-sponsored cyber intrusions.[14]

Counterterrorism Section (CTS)

- CTS leads DOJ on combating emerging and evolving terrorism threats in cyberspace.[15]

INTERPOL Washington

Operational Divisions (OD)

- OD works with domestic and foreign law enforcement partners to locate, apprehend, and return malicious cyber actors wanted by the United States who are in foreign countries and malicious cyber actors wanted by foreign countries in the United States. It also serves as a dedicated channel for exchanging cyber intelligence with the International Criminal Police Organization (INTERPOL).[16]

Office of the General Counsel (OGC)

- OGC is responsible for overseeing DOJ's Red (fugitive) Notice program, used to facilitate the return of international fugitives through INTERPOL and develops and reviews all agreements and Memoranda of Understanding between INTERPOL Washington and its partnering agencies.[17]

Federal Bureau of Investigation (FBI)

Criminal, Cyber, Response and Services Branch (CCRSB)

Cyber Division

- The Cyber Division at FBI Headquarters leads and coordinates the agency's efforts to investigate internet crimes, cyber-enabled terrorism, unauthorized computer intrusions, and cyber fraud.[18]

Cyber Action Teams

- Cyber Action Teams provide rapid incident response on major computer intrusions and cyber-related emergences around the globe, including gathering vital intelligence in cybercrime investigations.[19]

Cyber Watch (CyWatch)

- CyWatch is the FBI's 24-hour command center responsible for coordinating domestic law enforcement response to criminal and national security cyber intrusions, tracking victim notification, and coordinating with other federal cyber centers.[20]

National Cyber Investigative Joint Task Force (NCIJTF)

- The NCIJTF is a multi-agency task force led by the FBI with the primary responsibility to coordinate, integrate, and share information to support cyber threat investigations, supply and support intelligence analysis for community decision-makers on cyber threats, and synchronize joint efforts across the different agencies.[21]

iGuardian

- iGuardian is a secure portal allowing FBI partners within critical telecommunications, defense, banking and finance, and energy infrastructure sectors to report cyber intrusion incidents to the FBI in real time.[22]

Internet Crime Complaint Center (IC3)

- The IC3 is the FBI's public reporting mechanism on internet-facilitated criminal activity, which allows the FBI to receive, develop, and refer criminal complaints regarding cybercrime.[23]

National Cyber Forensics & Training Alliance (NCFTA)

- The NCFTA brings together law enforcement, private industry, and academia to share information to stop emerging cyber threats and mitigate existing ones.[24]

Cyber Initiative and Resource Fusion Unit (CIRFU)

- CIRFU is the cyber unit attached to the NCFTA and analyzes cyber threats and eliminates false leads before cyber cases are referred to other law enforcement agencies.[25]

International Operations Division

Legal Attaché (Legat) Program

- Legal attaché offices or Legats are FBI offices located in US embassies abroad where stationed special agents and other overseas personnel can assist international law enforcement partners in their response to and investigation of cybercrimes.[26]

Science and Technology Branch

Operational Technology Division

National Domestic Communications Assistance Center (NDCAC)

- NDCAC is a hub for law enforcement and shares knowledge and resources on issues involving real-time and stored communications to address challenges posed by electronic evidence collection.[27]

U.S. Marshals Service (USMS)

Fugitive Apprehension Decision Unit

- The Fugitive Apprehension Decision Unit is authorized to investigate and apprehend fugitives in the United States and abroad, including cybercriminals wanted by US law enforcement.[28]

Asset Forfeiture Program

- The Asset Forfeiture Program has the authority to seize cryptocurrency (e.g., Bitcoin, Ether, and Monero) used by cybercriminals, which is vital for disrupting their criminal networks and recovering stolen assets.[29]

Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF)

- ATF has jurisdiction over the trafficking of explosive or incendiary devices, bomb threats, and firearms over the internet.[30]

State, Local, Tribal, and Territorial (SLTT) Law Enforcement Agencies

- SLTT law enforcement agencies work closely with their federal law enforcement counterparts to investigate cybercrime cases with a SLTT nexus.

United States Attorney's Offices (USAO)

- USAO's located nationwide work with DOJ to prosecute cybercrimes cases in their districts.

Department of Homeland Security

National Cybersecurity and Communications Integration Center (NCCIC)

- The NCCIC serves as the nation's 24/7 hub for cyber information, technical expertise, and cyber incident response.[31]

The United States Computer Emergency Readiness Team (US-CERT)

- US-CERT works with federal agencies, the private sector, the research community, and state and local governments by analyzing cyber incidents reported to the government, disseminating cyber threat warnings, and providing on-site incident response capabilities to federal and state agencies.[32]

U.S. Immigrations and Customs Enforcement (ICE)

Homeland Security Investigations (HSI)

- HSI has authority to investigate criminal activity conducted on or facilitated by the internet. Their Cyber Crime Center delivers computer-based technical services to support domestic and international investigations into cross-border crime conducted over the internet.[33]

United States Secret Service (USSS)

National Computer Forensics Institute (NCFI)

- The NCFI is the nation's only federally funded training center dedicated to instructing state and local law enforcement officers, prosecutors, and judges in cybercrime investigations.[34]

Electronic Crimes Task Forces (ECTFS)

- ECTFS are interagency task forces organized of USSS, state, local, and other federal law enforcement that conduct investigations into cryptocurrency, bank fraud, virus and worm proliferation, unauthorized device access, and a variety of other computer crimes.[35]

Electronic Crimes Special Agent Program (ECSAP)

- ECSAPs are located in USSS field offices across the country and are computer investigative specialists qualified to conduct examinations of all types of electronic evidence.[36]

Department of Treasury

Office of Terrorism and Financial Intelligence

Financial Crimes Enforcement Network (FinCEN)

- FinCEN works to identify sources of revenue for malicious cyber actors and their attempts to access and exploit international financial systems.[37] FinCEN uses and collects Suspicious Activity Reports (SARS) that financial institutions must submit as sources of intelligence and works with law enforcement to neutralize reported threats.

Office of Foreign Assets Control (OFAC)

- OFAC has the authority to issue economic and trade sanctions against persons engaging in significant malicious cyber-enabled activities and certain nation-state actors perpetrating malicious cyber activity against the United States.[38]

Internal Revenue Services (IRS)

Criminal Investigation (CI)

- CI is composed of financial investigators and all CI employees are required to complete cyber training. Special agents use specialized forensic technology to recover financial data that may have been encrypted, password protected, or hidden by other electronic means.[39]

Department of State

Bureau of International Narcotics and Law Enforcement (INL)

Office of Anti-crime Programs

- The Office of Anti-Crime Programs implements two programs to combat cybercrime: (1) a crime program that works with international partners to provide training and technical assistance aimed at strengthening law enforcement capacity to investigate and bring to justice cybercriminals; and (2) a criminal justice program that supports international law enforcement academies to strengthen international cooperation around cybercrime and other security threats.[40]

High Tech Crime Global Law Enforcement Network (GLEN)

- Through the GLEN, INL helps to coordinate and resource the network of International Computer Hacking and Intellectual Property Advisors (ICHIPS), which are DOJ attorneys located in key regions working to enhance their foreign law enforcement partners capacity to investigate and prosecute cyber and intellectual property crime.

Office of the Coordinator for Cyber Issues (S/CCI)[41]

- The Office was created in 2011 and coordinates the Departments' global diplomatic engagements on cyber issues. It has since been folded into the Bureau of Economic and Business Affairs.[42]

United States Agency for International Development (USAID)

- USAID, through its foreign assistance funding, implements a number of cybercrime capacity building programs through several of its regional and thematic bureaus.[43]

United States Postal Service (USPS)

US Postal Inspection Service

Cybercrime Unit (CU)

- The CU investigates and provides analytical support to criminal activities affecting the USPS computer networks and field investigations related to the dark web and cryptocurrencies.[44]

Federal Trade Commission (FTC)

Criminal Liaison Unit

- The Criminal Liaison Unit helps prosecutors bring criminal consumer fraud cases involving the internet, telemarketers, and identity theft. They train prosecutors and investigators on identifying suspects and witnesses using the Consumer Sentinel Network,[45] which is an online investigative tool available to law enforcement that contains consumer complaints involving a variety of fraud issues, including identity theft.[46]

Securities and Exchange Commission (SEC)

Enforcement Division

Cyber Unit

- The Cyber Unit works on cyber-related securities misconduct such as hacking to obtain material nonpublic information, misconduct perpetrated using the dark web, and intrusions into retail brokerage accounts.[47]

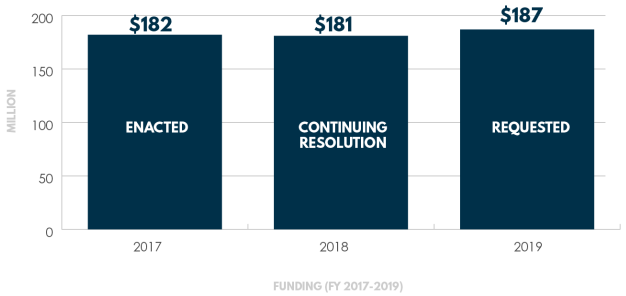
To reduce the cyber enforcement gap, Congress must evaluate whether key cyber enforcement entities have the necessary funding to make progress.

In order to make progress in reducing the cyber enforcement gap, Congress must evaluate whether the key entities involved in identifying, stopping, and bringing to justice malicious cyber actors have the required funding they need.

In order to assist Members of Congress and their staff in doing this evaluation during the FY 2020 budget process,[48] Third Way has compiled the budget history of key entities across the US government engaged in cyber enforcement (based on publicly available data). Only those entities whose budget levels are specifically listed in the Executive Branch's budget request and corresponding materials are included. As such, we were unable to ascertain funding levels for all of the specialized units and sections involved in cyber enforcement if their budgets are not made publicly available.

Department of Justice

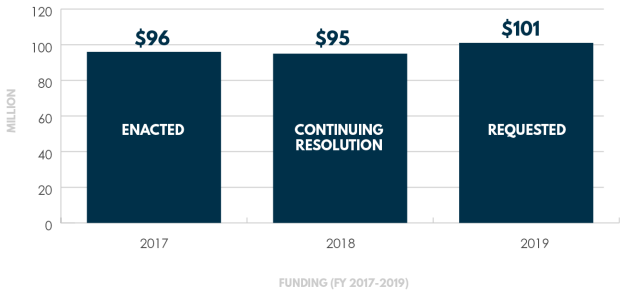
Criminal Division (CRM)



These figures are from the FY 2019 CRM CBJ for the entire Division because CRM does not provide funding information on individual Sections within the Division working on cyber enforcement.

Source: "FY 2019 Congressional Submission: Department of Justice Criminal Division." *Department of Justice*, Feb. 2018, pp. 17. www.justice.gov/jmd/page/file/1034256/download. Accessed 12 Feb. 2019.

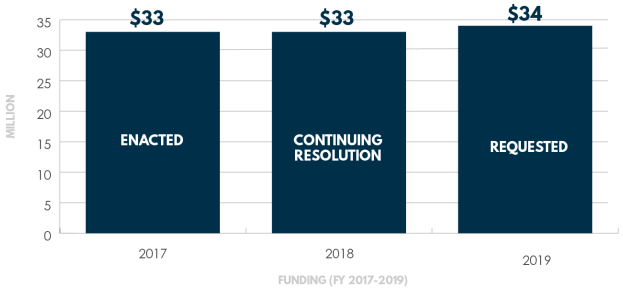
National Security Division



These figures are from the FY 2019 NSD CBJ and indicates the total funding for NSD and its combined Sections because NSD does not provide budget information on individual Sections working on cyber enforcement.

Source: "FY 2019 Performance Budget Congressional Justification National Security Division." *Department of Justice*, 2018, pp.12. www.justice.gov/jmd/page/file/1034226/download. Accessed 12 Feb. 2019.

INTERPOL Washington

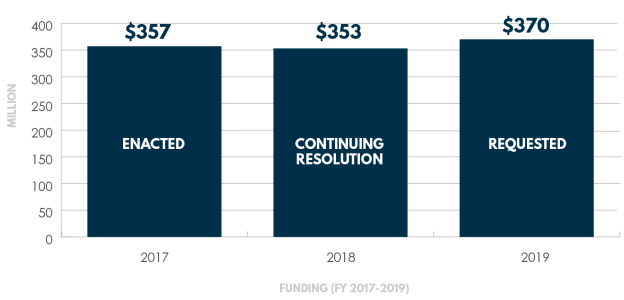


These figures are from the FY 2019 INTERPOL Washington CBJ as a total unit because INTERPOL Washington does not provide funding information on individual programs.

Source: "FY 2019 PERFORMANCE BUDGET: INTERPOL WASHINGTON U.S. NATIONAL CENTRAL BUREAU." *Department of Justice*, Feb. 2018, pp. 9. www.justice.gov/file/1034211/download. Accessed 12 Feb. 2019.

Federal Bureau of Investigation (FBI)

Cyber Budget

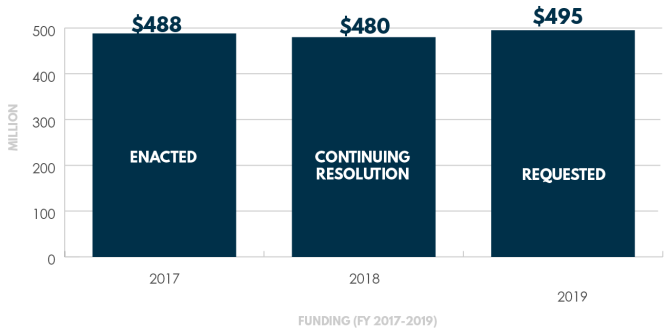


These figures are from FY 2019 FBI Authorization and Budget Request to Congress and includes all funding the FBI directs towards cyber investigations.

Source: "FY 2019 Authorization and Budget Request to Congress." *Federal Bureau of Investigation*, Feb. 2018, pp. 4-16. www.justice.gov/jmd/page/file/1034366/download. Accessed 12 Feb. 2019.

US Marshals Service (USMS)

Fugitive Apprehension



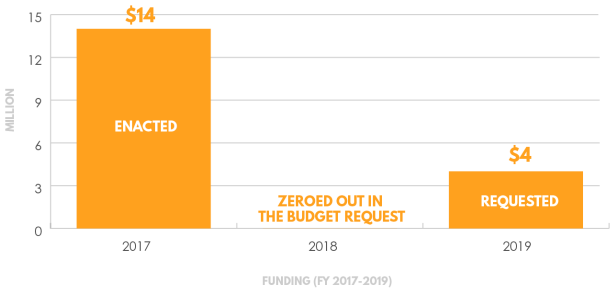
These figures are from the FY 2019 USMS Performance Budget and includes expenditures for domestic and international fugitive investigations.

Source: "United States Marshals Service FY 2019 Performance Budget President's Budget Salaries and Expenses Appropriation." *Department of Justice*, Feb. 2018, pp. 22. www.justice.gov/jmd/page/file/1034596/download. Accessed 12 Feb. 2019.

Department of Homeland Security

US Secret Service (USSS)

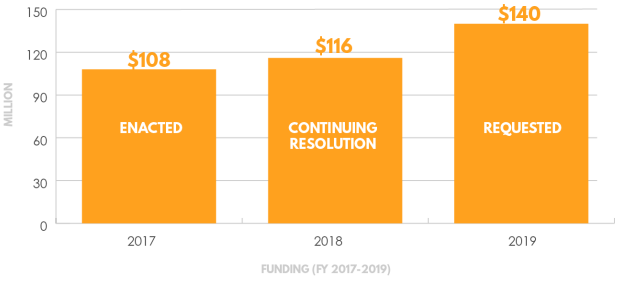
National Computer Forensic Institute (NCFI)



These figures are from the FY 2019 USSS CBJ and include expenditures for the nation's only federally funded law enforcement training center for cybercrime.

Source: "Fiscal Year 2019 Congressional Justification: Department of Homeland Security U.S. Secret Service Budget Overview." *Department of Homeland Security*, Feb. 2018, pp. O&S-89. www.dhs.gov/sites/default/files/publications/U.S.%20Secret%20Service.pdf. Accessed 12 Feb. 2019.

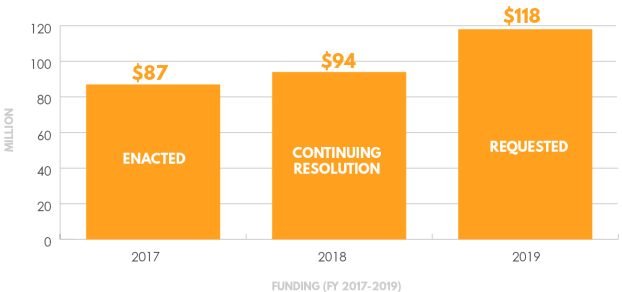
National Cybersecurity and Communications Integration Center (NCCIC)



These figures are from the FY 2019 National Protection and Programs Directorate CBJ and only includes figures for operational funding for the NCCIC. They do not include funding for planning and exercises, which cost between $84-88 million annually.

Source: "Fiscal Year 2019 Congressional Justification: Department of Homeland Security National Protection and Programs Directorate Budget Overview." *Department of Homeland Security*, Feb. 2018, pp. NPPD-18. www.dhs.gov/sites/default/files/publications/National%20Protection%20and%20Programs%20Directorate.pdf. Accessed 12 Feb. 2019.

Computer Emergency Readiness Team (US-CERT)

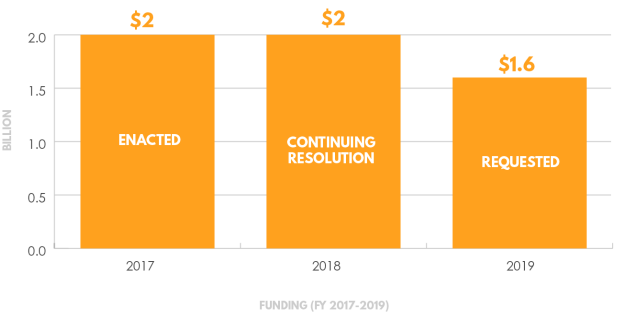


These figures are from the FY 2019 National Protection and Programs Directorate CBJ and only includes figures for operational funding for the CERT and does not include funding for planning and exercises, which is between $61-64 million annually.

Source: "Fiscal Year 2019 Congressional Justification: Department of Homeland Security National Protection and Programs Directorate Budget Overview." *Department of Homeland Security*, Feb. 2018, pp. NPPD-18. www.dhs.gov/sites/default/files/publications/National%20Protection%20and%20Programs%20Directorate.pdf. Accessed 12 Feb. 2019.

US Immigration and Customs Enforcement (ICE)

Homeland Security Investigations (HSI)

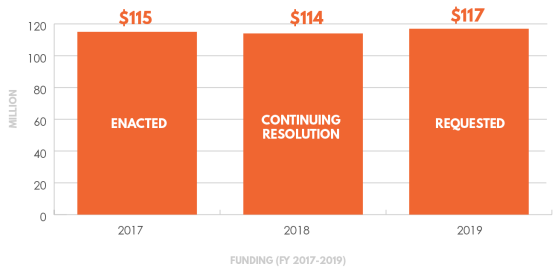


These figures are from the FY 2019 ICE CBJ and includes amounts for HSI's: (1) domestic investigations, (2) international operations, and (3) intelligence.

Source: "Fiscal Year 2019 Congressional Justification: Department of Homeland Security." *Department of Homeland Security, U.S. Immigration and Customs Enforcement*, Feb. 2018, pp. O&S-54. www.dhs.gov/sites/default/files/publications/U.S.%20Immigration%20and%20Customs%20Enforcement.pdf. Accessed 12 Feb. 2019.

Department of Treasury

Financial Crimes Enforcement Network (FinCEN)

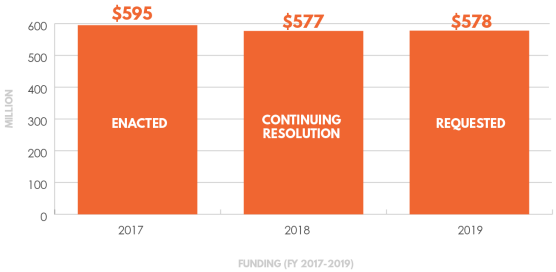


These figures are from the FY 2019 FinCEN CBJ and includes all funds allocated to the Network.

Source: "FY 2019 Congressional Budget Justification and Annual Performance Report and Plan Financial Crimes Enforcement Network." *Department of the Treasury*, Feb. 2018, pp.FinCEn-7. https://www.treasury.gov/about/budget-performance/CJ19/14.%20FinCEN%20FY%202019%20CJ.pdf. Accessed 12 Feb. 2019.

International Revenue Services (IRS)

Criminal Investigations (CI)



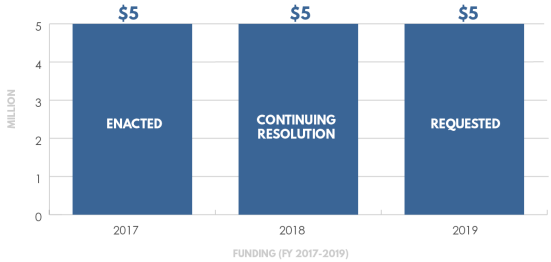
These figures are for the FY 2019 IRS CBJ and include all funds allocated towards criminal investigations.

Source: "FY 2019 Congressional Budget Justification and Annual Performance Report and Plan Internal Revenue Service." Department of the Treasury, Feb. 2018, pp.IRS-40.https://www.treasury.gov/about/budget-performance/CJ19/05.%20IRS%20FY%202019%20CJ.pdf. Accessed 12 Feb. 2019.

Department of State

Bureau of International Narcotics and Law Enforcement Affairs

Cyber Crime and Intellectual Property Rights

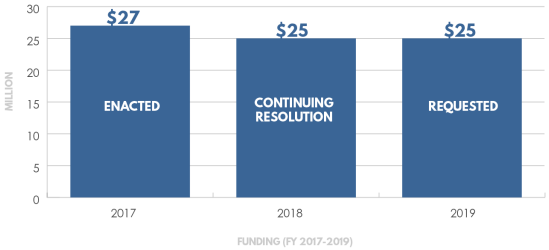


These figures are from the FY 2019 Department of State, Foreign Operations, and Related Programs CBJ and include funds INL directs towards cybercrime capacity building.

Source: "Congressional Budget Justification: Department of State, Foreign Operations, and Related Programs." *Department of State*, 12 Feb. 2018, pp. 144. www.state.gov/documents/organization/277155.pdf. Accessed 12 Feb. 2019.

Bureau of International Narcotics and Law Enforcement Affairs

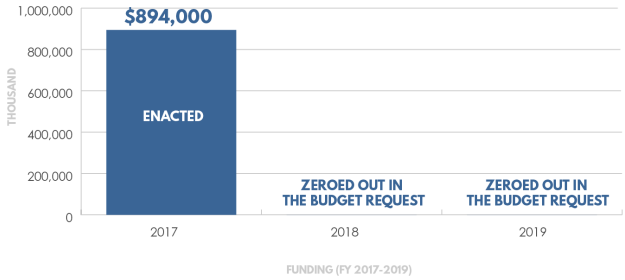
International Law Enforcement Academy



These figures are from the FY 2019 Department of State, Foreign Operations, and Related Programs CBJ and includes funds INL directs towards cybercrime capacity building.

Source: "Congressional Budget Justification: Department of State, Foreign Operations, and Related Programs." *Department of State*, 12 Feb. 2018, pp. 144. www.state.gov/documents/organization/277155.pdf. Accessed 12 Feb. 2019.

Office of the Coordinator for Cyber Issues



These figures are from the FY 2019 Department of State, Foreign Operations, and Related Programs CBJ. The Office has been merged into the Bureau of Economic and Business Affairs.

Source: "Congressional Budget Justification: Department of State, Foreign Operations, and Related Programs." *Department of State*, 12 Feb. 2018, pp. 144. www.state.gov/documents/organization/277155.pdf. Accessed 12 Feb. 2019.

Overall, funding for key cyber enforcement entities has remained consistent with a few increases from FY 2017-2019. However, in previous years the Trump Administration has requested to eliminate funding for the National Computer Forensic Institute (NCFI). Congress should work to ensure it has sufficient funding to fulfill its mandate. Even at its height, the NCFI was only running at about one-third capacity and would require close to $35 million to be at full capacity [49] — far from the $4 million currently budgeted. Further, dedicated funding for the State Department's Office of the Coordinator for Cyber Issues has been eliminated from the budget request, which should be re-established along with the authorization for the Office led by an Ambassador.

Although overall funding for cyber enforcement has largely been consistent, what is clear is that the current allocation of funding is not enough to reduce the cyber enforcement gap—particularly for entities like the FBI, USSS, and the State Department's INL Bureau. Congress should evaluate whether strategic boosts in funding for certain key US entities involved in cyber enforcement are necessary in order to provide them with the resources needed to stop, identify, and punish malicious cyber actors and put a large dent in the cyber enforcement gap.

Conclusion

The United States is facing a cybercrime wave, and based on our research less than 1% of these crimes ever see an arrest of the perpetrator—a large cyber enforcement gap. There are a multitude of government entities with the responsibility to reduce this cyber enforcement gap, including federal, state, and local law enforcement agencies and the Department of State. Yet, despite the number of entities involved in cyber enforcement, the cyber enforcement gap remains large. When reviewing the FY 2020 budget from the Trump Administration, Members of Congress and their staff should familiarize themselves with the scope of entities involved in cyber enforcement and assess whether they have sufficient funding to make progress.

ENDNOTES

1 Eoyang, Mieke, et al. "To Catch a Hacker: Toward a Comprehensive Strategy to Identify, Pursue, and Punish Malicious Cyber Actors." Third Way, Third Way, 29 Oct. 2018, pp. 1-2. https://thirdway.imgix.net/pdfs/override/To_Catch_Hacker_Report_FINAL.pdf. Accessed 12 Feb. 2019.

2 Eoyang, Mieke, et al. "To Catch a Hacker: Toward a Comprehensive Strategy to Identify, Pursue, and Punish Malicious Cyber Actors." Third Way, Third Way, 29 Oct. 2018, pp. 1-2. https://thirdway.imgix.net/pdfs/override/To_Catch_Hacker_Report_FINAL.pdf. Accessed 12 Feb. 2019.

3 Eoyang, Mieke, et al. "Third Way Cyber Enforcement Initiative." Third Way, Third Way. https://www.thirdway.org/series/third-way-cyber-enforcement-initiative. Accessed 12 Feb. 2019.

4 Eoyang, Mieke, et al. "To Catch a Hacker: Toward a Comprehensive Strategy to Identify, Pursue, and Punish Malicious Cyber Actors." Third Way, Third Way, 29 Oct. 2018, pp. 1-2. https://thirdway.imgix.net/pdfs/override/To_Catch_Hacker_Report_FINAL.pdf. Accessed 12 Feb. 2019.

5 Eoyang, Mieke, et al. "To Catch a Hacker: Toward a Comprehensive Strategy to Identify, Pursue, and Punish Malicious Cyber Actors." Third Way, Third Way, 29 Oct. 2018, pp. 25. https://thirdway.imgix.net/pdfs/override/To_Catch_Hacker_Report_FINAL.pdf. Accessed 12 Feb. 2019.

6 For example, there are Inspector General Offices in various agencies that investigate cybercrimes at their respective agencies that were not included in this list. Additionally, the US Intelligence Community (IC) supports law enforcement efforts on malicious cyber activity through intelligence sharing but the scope of entities in the IC was not assessed.

7 "Cybersecurity Unit." Department of Justice, 16 Oct. 2018. www.justice.gov/criminal-ccips/cybersecurity-unit. Accessed 12 Feb. 2019.

8 "About OCGS." Department of Justice, 26 May 2015. www.justice.gov/criminal-ocgs/about-ocgs. Accessed 12 Feb. 2019.

9 "Money Laundering and Asset Recovery Section (MLARS)." Department of Justice, 2 Jan. 2019. www.justice.gov/criminal-mlars. Accessed 12 Feb. 2019.

10 "Office of International Affairs (OIA)." Department of Justice, 18 Sept. 2018, www.justice.gov/criminal-oia. Accessed 12 Feb. 2019.

11 "Office of Overseas Prosecutorial Development Assistance and Training (OPDAT)." Department of Justice, 26 Feb. 2018, www.justice.gov/criminal-opdat. Accessed 12 Feb. 2019.

12 "About ICITAP." Department of Justice, 22 Oct. 2018. www.justice.gov/criminal-icitap/about-icitap. Accessed 12 Feb. 2019.

13 "Attorney General Loretta E. Lynch Delivers Remarks at National Security Division 10-Year Anniversary Event." Department of Justice, 12 Dec. 2016. www.justice.gov/opa/speech/attorney-general-loretta-e-lynch-delivers-remarks-national-security-division-10-year. Accessed 12 Feb. 2019.

14 "FY 2019 Performance Budget Congressional Justification National Security Division." Department of Justice, 2018, pp.3. www.justice.gov/jmd/page/file/1034226/download. Accessed 12 Feb. 2019.

15 "FY 2019 Performance Budget Congressional Justification National Security Division." Department of Justice, 2018, pp.2. www.justice.gov/jmd/page/file/1034226/download. Accessed 12 Feb. 2019.

16 "Divisions." Department of Justice, Department of Justice, 24 Apr. 2018, www.justice.gov/interpol-washington/divisions. Accessed 12 Feb. 2019.

17 "Divisions." Department of Justice, Department of Justice, 24 Apr. 2018, www.justice.gov/interpol-washington/divisions. Accessed 12 Feb. 2019.

18 "Cyber Crime." FBI, Federal Bureau of Investigation, 26 Sept. 2018, www.fbi.gov/investigate/cyber. Accessed 12 Feb. 2019.

19 "Cyber Crime." FBI, Federal Bureau of Investigation, 26 Sept. 2018. www.fbi.gov/investigate/cyber. Accessed 12 Feb. 2019.

20 Smith, Scott. "Roles and Responsibilities for Defending the Nation from Cyber Attack." FBI, Federal Bureau of Investigation, 19 Oct. 2017. www.fbi.gov/news/testimony/cyber-roles-and-responsibilities. Accessed 12 Feb. 2019.

21 "National Cyber Investigative Joint Task Force." FBI, Federal Bureau of Investigation, 13 June 2016. www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force. Accessed 12 Feb. 2019.

22 "IGuardian." FBI, Federal Bureau of Investigation, 22 July 2016. www.fbi.gov/resources/law-enforcement/iguardian. Accessed 12 Feb. 2019.

23 "IC3 Mission Statement." Federal Bureau of Investigation Internet Crime Complaint Center, Federal Bureau of Investigation. www.ic3.gov/about/default.aspx. Accessed 12 Feb. 2019.

24 "The NCFTA: Combining Forces to Fight Cyber Crime." FBI, Federal Bureau of Investigation, 16 Sept. 2011, www.fbi.gov/news/stories/the-ncfta-combining-forces-to-fight-cyber-crime. Accessed 12 Feb. 2019.

25 "The NCFTA: Combining Forces to Fight Cyber Crime." FBI, Federal Bureau of Investigation, 16 Sept. 2011, www.fbi.gov/news/stories/the-ncfta-combining-forces-to-fight-cyber-crime. Accessed 12 Feb. 2019.

26 "FY 2019 Authorization and Budget Request to Congress." Federal Bureau of Investigation, Feb. 2018, pp. 4-11-12. www.justice.gov/jmd/page/file/1034366/download. Accessed 12 Feb. 2019.

27 "REPORT OF THE ATTORNEY GENERAL'S CYBER DIGITAL TASK FORCE." Department of Justice, 2 July 2018, pp.87. www.justice.gov/ag/page/file/1076696/download. Accessed 12 Feb. 2019.

28 "Fact Sheet Fugitive Apprehension 2018." Department of Justice. 13 Apr. 2018. www.usmarshals.gov/duties/factsheets/fugitive_ops.pdf. Accessed 12 Feb. 2019.

29 "REPORT OF THE ATTORNEY GENERAL'S CYBER DIGITAL TASK FORCE." Department of Justice, 2 July 2018, pp. 54-55. www.justice.gov/ag/page/file/1076696/download. Accessed 12 Feb. 2019.

30 "Reporting Computer, Internet-Related, Or Intellectual Property Crime." The United States Department of Justice, The United States Department of Justice, 18 Dec. 2018. www.justice.gov/criminal-ccips/reporting-computer-internet-related-or-intellectual-property-crime. Accessed 12 Feb. 2019.

31 "About Us." Cybersecurity and Infrastructure Security Agency, Department of Homeland Security. www.us-cert.gov/about-us. Accessed 12 Feb. 2019.

32 "United States Computer Emergency Readiness Team." Department of Homeland Security. www.us-cert.gov/sites/default/files/publications/infosheet_US-CERT_v2.pdf. Accessed 12 Feb. 2019.

33 "Cyber Crimes Center." ICE, Department of Homeland Security. www.ice.gov/cyber-crimes. Accessed 12 Feb. 2019.

34 "Fiscal Year 2019 Congressional Justification: Department of Homeland Security U.S. Secret Service Budget Overview." Department of Homeland Security, Feb. 2018, pp. O&S-18. www.dhs.gov/sites/default/files/publications/U.S.%20Secret%20Service.pdf. Accessed 12 Feb. 2019.

35 "United States Secret Service Electronic Crimes Task Forces." United States Secret Service. www.dhs.gov/sites/default/files/publications/USSS_Electronic-Crimes-TaskForces.pdf. Accessed 12 Feb. 2019.

36 "Fiscal Year 2019 Congressional Justification: Department of Homeland Security U.S. Secret Service Budget Overview." Department of Homeland Security, Feb. 2018, pp. O&S-76. www.dhs.gov/sites/default/files/publications/U.S.%20Secret%20Service.pdf. Accessed 12 Feb. 2019.

37 "FY 2019 Congressional Budget Justification and Annual Performance Report and Plan Financial Crimes Enforcement Network." Department of the Treasury, Feb. 2018. www.treasury.gov/about/budget-performance/CJ19/14.%20FinCEN%20FY%202019%20CJ.pdf. Accessed 12 Feb. 2019.

38 "Office of Foreign Asset Control: CYBER-RELATED SANCTIONS PROGRAM." Department of the Treasury, 3 July 2017. www.treasury.gov/resource-center/sanctions/Programs/Documents/cyber.pdf. Accessed 12 Feb. 2019.

39 "Criminal Investigation (CI) At a Glance." Internal Revenue Service, Internal Revenue Service, 25 July 2018. www.irs.gov/about-irs/criminal-investigation-ci-at-a-glance. Accessed 12 Feb. 2019.

40 "Office of Anti-Crime Programs (INL/C)." U.S. Department of State, U.S. Department of State. https://2009-2017.state.gov/j/inl/c/index.htm. Accessed 12 Feb. 2019.

41 Currently, the Office of the Cyber Coordinator for Cyber Issues has been folded into the Division of International Communications and Information within the Bureau of Economic and Business Affairs. Congressional legislation has been introduced to establish an Office of International Cyberspace Policy at the State Department, with the office reporting to the undersecretary of state for political affairs. Source: Groll, Elias, and Robbie Gramer. "New Bill Seeks to Energize American Cyberdiplomacy." Foreign Policy, Foreign Policy, 24 Jan. 2019, foreignpolicy.com/2019/01/24/new-bill-seeks-to-energize-american-cyberdiplomacy/. Accessed 12 Feb. 2019.

42 "Office of the Coordinator for Cyber Issues." U.S. Department of State, U.S. Department of State. www.state.gov/s/cyberissues/. Accessed 12 Feb. 2019.

43 "JOINT STRATEGIC PLAN FY 2018 - 2022." U.S. Department of State & U.S. Agency for International Development, Feb. 2018. www.usaid.gov/sites/default/files/documents/1870/JSP_FY_2018_-_2022_FINAL.pdf. Accessed 12 Feb. 2019.

44 "FY 2019 Annual Report US Postal Inspection Service." United States Postal Service, pp. 12-13. https://postalinspectors.uspis.gov/radDocs/AR2017.pdf. Accessed 12 Feb. 2019.

45 "Criminal Liaison Unit." Federal Trade Commission, Federal Trade Commission, 25 Feb. 2015. www.ftc.gov/enforcement/criminal-liaison-unit. Accessed 12 Feb. 2019.

46 "THE FTC'S CONSUMER SENTINEL NETWORK." Federal Trade Commission. www.ftc.gov/sites/default/files/attachments/consumer-sentinel-network/factsheet.pdf. Accessed 12 Feb. 2019.

47 "SEC Announces Enforcement Initiatives to Combat Cyber-Based Threats and Protect Retail Investors." Securities and Exchange Commission, Securities and Exchange Commission, 25 Sept. 2017. www.sec.gov/news/press-release/2017-176. Accessed 12 Feb. 2019.

48 The recent federal shutdown has caused a delay in the release of the FY 2020 federal budget and the lack of a regular budget process may impact the ability of departments and agencies to report their FY 2019 enacted budget amounts. Therefore, budget numbers reported here are for FY 2019 "requested" amounts rather than "enacted" amounts due to these delays.

49 Carter, William A, and Jennifer C Daskal. "Low-Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge." Center for Strategic and International Studies, July 2018, pp. 14-15. csis-prod.s3.amazonaws.com/s3fs-public/publication/180725_Carter_DigitalEvidence.pdf?tAGR_DvxRdp0RspiGYNGcGKTUjrGY3rN. Accessed 12 Feb. 2019.