Appendix: Cybercrime Policy Actions

This appendix includes publicly-available policy actions taken by relevant executive branch departments and agencies since 2018 to combat cybercrime. Most of these actions were presumably driven by the White House's "National Cyber Strategy," which was released in 2018 and outlined the Administration's planned efforts to reduce cybercrime, among other priorities. The agencies and departments listed below are not a holistic list of all the federal entities with cybercrime enforcement missions, nor is it a complete list of every action taken by these entities on cybercrime. For example, indictments and sanctions are not included in this overview. Further, in an effort to focus solely on federal actions, important Congressional legislation has not been included, such as the CLOUD Act and measures introduced in National Defense Authorization Acts, that impact cybercrime enforcement.

DEPARTMENT OF HOMELAND SECURITY

DHS Cybersecurity Strategy[1]

Description: This five-year strategy outlines DHS' cybercrime goals and objectives. The objectives include combating financial and international cybercrimes, preventing and disrupting cybersecurity threats to protected persons and critical infrastructure, increasing law enforcement capacity, and enhancing investigative abilities.

Homeland Security Investigations: Cybercrime Symposium[2]

Description: In April 2019, HSI held a cybercrime symposium with 200 law enforcement personnel from state, local, and federal partners to highlight HSI's cybercrime capabilities and forge partnerships. Topics included typologies of cyber criminal's technology vs. human-based attacks, technological capabilities for case support and unique challenges in the digital world, interagency cooperation and international partnerships, and others.

THE 2020-2024 DHS STRATEGIC PLAN[3]

Description: This four-year strategy for DHS details one objective on combating cybercrime and five relevant sub-objectives that mostly reiterate the objectives in the DHS' 2018 Cybersecurity Strategy.[4] The Strategy's objectives include

investigating cybercrime consistent with DHS authorities, providing cyber investigative assistance to domestic and foreign partners, and investigating transnational cybercrime.

DEPARTMENT OF JUSTICE

Attorney General Barr's Memo Prioritizing Cybercrime Prosecutions[5]

Description: In March 2020, the Attorney General of the United States issued a memo to all US Attorneys to prioritize cybercrime prosecutions stemming from the COVID-19 pandemic, directing all US Attorneys to "prioritize the detection, investigation, and prosecution of all criminal conduct related to the pandemic." It also encourages these offices to collaborate with state and local law enforcement.

Connecticut, Delaware, Virginia, and West Virginia Coronavirus Fraud Task Force[6]

Description: In March and April 2020, DOJ formed task forces with these four states to identify, investigate, and prosecute fraud and cybercrime related to the ongoing COVID-19 pandemic in their respective states. These task forces are composed of representatives from DOJ, the FBI, DHS's Homeland Security Investigations (HSI), the Internal Revenue Service (IRS)-Criminal Investigation (CI), and the state's relevant law enforcement agencies.

Cybercrime Symposiums in 2018 and 2020[7]

Description: DOJ has held a series of cybercrime symposiums with Academic partners, with one being held in 2018 and one in 2020, to discuss cybercrime trends, lessons learned, and challenges with practitioners and subject matter experts.

Cybersecurity Industry Roundtable[8]

Description: In September 2018, the DOJ's Criminal Division hosted a roundtable with federal law enforcement agencies and private sector partners to discuss challenges with data breach investigations. The roundtable convened officials from the FBI, US Secret Service, the National Security Council, DHS, and private sector participants to share best practices, common challenges, and emerging threats on data breaches.

DOJ's 2018-2022 Strategic Plan[9]

Description: In 2018, DOJ issued this four-year strategy that, among other things, included a series of goals and objectives to deter "cyber-based threats and attacks." To combat cyber threats, the plan calls upon DOJ to (1) identify, disrupt, and prosecute cyber threat actors; (2) develop and use all appropriate tools to

identify and disrupt cyber threats; and (3) strengthen public-private partnerships.

DOJ and Private Sector Partnership to Disrupt Online Domains[10]

Description: In April 2020, multiple federal law enforcement agencies announced an ongoing cooperation between themselves and private sector companies managing or hosting internet websites (domains and registrars) to disrupt domains that are being used for criminal purposes.

DOJ Initiative to Combat Chinese Economic Espionage[11]

Description and Details: In November 2018, the US Attorney General launched an initiative to prioritize Chinese trade theft cases and to ensure that DOJ had sufficient resources to pursue these cases.

Report of the Attorney General's Cyber Digital Task Force[12]

Description: The DOJ released this report to highlight their challenges in reducing cybercrime and proposed solutions. Challenges to the DOJ's efforts to combat cybercrime include working with the private sector; investigating and prosecuting cybercrime; and other legal actions to dismantle, disrupt, and deter malicious cyber conduct.

DEPARTMENT OF STATE

Bilateral Engagements

Description: In addition to multilateral engagements through the United Nations and other international forums, the State Department also engaged in bilateral activities with the Netherlands, Estonia, and others to establish agreed upon norms and standards. [13]

Capacity Building Actions

Description: A core tenet of the State Department's cybercrime enforcement work is bolstering the capacity and capabilities of foreign criminal justice actors.[14] The Department has hosted cybercrime capacity building workshops with other nations and dedicated technical assistance funding.[15] The State Department also regularly gives contributions to international organizations for cybercrime cooperation and capacity building efforts, including a $500,000 contribution to the Organization of American States (OAS) Cybercrime Program over for cybercrime training and technical assistance.[16] Its Bureau of International Narcotics and Law Enforcement has also resourced and coordinated with DOJ the Global Law Enforcement Network (GLEN) of International Computer Hacking and Intellectual Property (ICHIP) attorney advisors, which in 2018 was

consolidated to place attorneys overseas at US embassies and consulates to advise on national and regional cyber legal issues.[17]

Condemnations and Warnings

Description: At times, the State Department will use the bully pulpit to condemn certain state and non-state actions in cyberspace to reiterate that nation-states must adhere to international laws, norms, and standards. For example, the State Department used this tool on two separate occasions against the Russians and those responsible for attacks against the Czech Republic's healthcare sector.[18]

Recommendations to the President on Deterring Adversaries and Better Protecting the American People and on Protecting American Cyber Interests through International Engagement Office of the Coordination [19]

Description: The State Department provided the President these two sets of recommendations on how it could deter malicious actors in cyberspace and enhance international engagement. Recommendations to combat cybercrime included "[c]riminal charges and prosecutions as well as tools such as sanctions can be used to deter most would-be malicious actors" and "[engaging in] a range of forms from direct diplomatic action, to include diplomacy and foreign assistance, and joint military exercises to participation in policy and technical standard-setting bodies alongside non-governmental stakeholders."

Resolutions and Statements through International Forums

Description: The State Department engages in various international forums[20] to gain consensus and signatures on joint resolutions, statements, and other documents to deter cybercriminals. It also focuses on building partnerships for increased cooperation in response to malicious cyber activity. For example, the State Department announced that it would work with partner nations to increase consequences on nations that misbehave in cyberspace.[21] The State Department also jointly issued a statement with 26 nations endorsing the importance of rules-based order and supported efforts at the UN to develop norms for responsive state behavior in cyberspace that includes components on cybercrime cooperation. However, the State Department unsuccessfully opposed a Russian-drafted UN resolution to develop a new global convention on countering the use of ICTs for criminal purposes.[22]

State and USAID Joint Strategic Plan for FY2018-2022[23]

Description: This four-year strategy includes a goal for increasing international cooperation to secure cyberspace and strengthen the capacity of the United States and partner nations to respond to international cyber threats. Specifically, it calls upon the State Department to "build a coalition of like-minded governments to identify and hold regimes accountable for engaging in or permitting malicious cyber activities to occur on their territory."

FEDERAL BUREAU OF INVESTIGATIONS

Investigation Model Restructured[24]

Description: In April 2019, the FBI restructured its investigative model to improve efficiency by identifying a lead office to coordinate other offices when a new cyber threat actor or malware strain becomes active. FBI headquarters will also now aggregate cybercrime intelligence and share it with relevant agencies.

Ransomware Summit[25]

Description: In September 2019, the FBI held a closed-door summit with cyber insurance companies, top private sector executives, and others to close intelligence gaps on ransomware threats. This forum allowed private sector executives to identify the type of information they should send to the FBI to aid ransomware investigations and for the FBI to provide a brief on current ransomware crimes.

UNITED STATES SECRET SERVICE

Cyber Investigations Advisory Board[26]

Description: The Secret Service selected a group of private-sector cybersecurity professionals to advise the agency's investigations team on improving their ability to take down cybercriminals. Sixteen members will join the advisory committee to help the investigative unit "think outside the box" in fighting cybercrime. The members come from industry, academia, and state and local governments.

Proposed USSS Move to the Treasury Department[27]

The President's FY 2021 budget includes a proposal to move the Secret Service from DHS back to the Department of Treasury to bolster cybercrime enforcement. The proposal cites the "increasing interconnectedness of the international financial marketplace have resulted in more complex criminal organizations and revealed stronger links between financial and electronic crimes and the financing of terrorists and rogue state actors" for the move.

National Seminar for Cyber Incident Response[28]

Description: In May 2019, the Secret Service's Electronic Crimes Task Forces held an inaugural National Seminar for Cyber Incident Response with public and

private partners to address collaboration gaps. Attendees discussed information and collaboration gaps that exist in cybersecurity; the complex cyber-threat environment; the needs of organizations victimized by cybercrime; and the capabilities, investigative processes and tools of the Secret Service, as well as held a cybercrime simulation exercise.

ENDNOTES

[1] United States Department of Homeland Security. "Cybersecurity Strategy." 15 May, 2018, https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf. Accessed 11 May 2020.

[2] "HSI New York hosts 1st annual Cyber Crime Symposium." Press Release, United States Department of Homeland Security, Immigrations and Customs Enforcement, 19 Apr. 2019, https://www.ice.gov/news/releases/hsi-new-york-hosts-1st-annual-cyber-crime-symposium. Accessed 11 May 2020.

[3] United States Department of Homeland Security. "The DHS Strategic Plan Fiscal Years 2020 - 2024." https://www.dhs.gov/sites/default/files/publications/19_0702_plcy_dhs-strategic-plan-fy20-24.pdf. Accessed 11 May 2020.

[4] While this strategy was created prior to the National Cyber Strategy, it offers insight into what type of policies DHS will create. United States Department of Homeland Security. "Cybersecurity Strategy." 15 May, 2018, https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf. Accessed 11 May 2020.

[5] William Barr. "COVID-19 - Department of Justice Priorities." *United States Office of the Attorney General*, 16 Mar. 2020, http://www.documentcloud.org/documents/6811684-Bill-Barr-DOJ-Priorities-Coronavirus-Scams.html. Accessed 11 May 2020.

[6] "Connecticut Announces Joint Federal-State COVID-19 Fraud Task Force." Press Release, *United States Department of Justice, U.S. Attorney's Office, District of Columbia*, 6 May 2020, https://www.justice.gov/usao-ct/pr/connecticut-announces-joint-federal-state-covid-19-fraud-task-force. Accessed 11 May 2020; "Top Federal and State Prosecutors Form Delaware COVID-19 Anti-Fraud Coalition." Press Release, *United States Department of Justice, U.S. Attorney's Office, District of Delaware*, 24 Apr 2020, https://www.justice.gov/usao-de/pr/top-federal-and-state-prosecutors-form-delaware-covid-19-anti-fraud-coalition. Accessed 11 May 2020; "Federal and State Officials Launch Virginia Coronavirus Fraud Task Force." Press Release, *United States Department of Justice, U.S. Attorney's Office, Western District of Virginia*, 20 Mar. 2020, https://www.justice.gov/usao-wdva/pr/federal-and-state-officials-launch-virginia-coronavirus-fraud-task-force. Accessed 11 May 2020; "Federal and State Officials Launch West Virginia Coronavirus Fraud Task Force." Press Release, *United States Department of Justice, U.S. Attorney's Office, Northern District of West Virginia,* 31 Mar. 2020, https://www.justice.gov/usao-ndwv/pr/federal-and-state-officials-launch-west-virginia-coronavirus-fraud-task-force. Accessed 11 May 2020.

[7] "Cybercrime Symposium." Department of Justice. https://www.justice.gov/criminal-ccips/cybercrime-symposium Accessed 11 May 2020.

[8] "Justice Department Hosts Cybersecurity Industry Roundtable." Press Release, *United States Department of Justice, Office of Public Affairs,* 28 Sep. 2018,

https://www.justice.gov/opa/pr/justice-department-hosts-cybersecurity-industry-roundtable. Accessed 11 May 2020.

[9]While this strategy was created prior to the National Cyber Strategy, it offers insight into what type of policies the Department of Justice will create. United States Department of Justice. "DOJ Strategic Plan for Fiscal Years 2018 - 2022." Feb. 2018, https://www.justice.gov/jmd/page/file/1071066/download. Accessed 11 May 2020.

[10] "Department of Justice Announces Disruption of Hundreds of Online COVID-19 Related Scams." Press Release, *United States Department of Justice, Office of Public Affairs*, 22 Apr. 2020, https://www.justice.gov/opa/pr/department-justice-announces-disruption-hundreds-online-covid-19-related-scams. Accessed 11 May 2020.

[11] "Attorney General Jeff Sessions Announces New Initiative to Combat Chinese Economic Espionage." Remarks as prepared for delivery, *United States Department of Justice, Office of Public Affairs*, 1 Nov. 2018, https://www.justice.gov/opa/speech/attorney-general-jeff-sessions-announces-new-initiative-combat-chinese-economic-espionage. Accessed 11 May 2020.

[12] Deputy Attorney General Rod Rosenstein. "Report of the Attorney General's Cyber Digital Taskforce." *United States Department of Justice*, 2 July 2018, https://www.justice.gov/ag/page/file/1076696/download. Accessed 11 May 2018.

[13] "Joint Statement on the Inaugural U.S.-Dutch Cyber Dialogue." Media Note, *United States Department of State, Office of the Spokesperson*, 20 May 2019, https://www.state.gov/joint-statement-on-the-inaugural-u-s-dutch-cyber-dialogue/. Accessed 12 May 2020; "Joint Statement on the Third U.S.-Estonia Cyber Dialogue." Media Note, *United States Department of State, Office of the Spokesperson*, 7 June 2019, https://www.state.gov/joint-statement-on-the-third-u-s-estonia-cyber-dialogue/. Accessed 12 May 2020.

[14] United States Department of State, United States Agency for International Development. "Joint Strategic Plan FY 2018 - 2022." Feb 2018. https://www.state.gov/wp-content/uploads/2018/12/Joint-Strategic-Plan-FY-2018-2022.pdf. Accessed 11 May 2020.

[15] "The United States Holds Inaugural Cyber Capacity Building Workshop for the Caribbean and Latin America." Media Note, *United States Department of State, Office of the Spokesperson*, 5 Dec. 2019, https://www.state.gov/the-united-states-holds-inaugural-cyber-capacity-building-workshop-for-the-caribbean-and-latin-america/. Accessed 11 May 2020; United States Department of State. "Cyber Successes: Highlights of 2019 and Look Ahead to 2020." *United States Department of State*, 10 Jan. 2019, https://www.state.gov/cyber-successes-highlights-of-2019-and-look-ahead-to-2020/. Accessed 11 May 2020.

[16] "United States Fights Cybercrime With Contribution to Organization of American States Program." Media Note. *United States Department of State, Office of the Spokesperson*, 29 Oct. 2019, https://www.state.gov/united-states-fights-cybercrime-with-contribution-to-organization-of-american-states-program/. Accessed 11 May 2020.

[17] "Overseas Work" Department of Justice. https://www.justice.gov/criminal-ccips/overseas-work Accessed 11 May 2020.

[18] "The United States Condemns Russian Cyber Attack Against the Country of Georgia." Press Statement, *United States Department of State*, 20 Feb. 2020, https://www.state.gov/the-united-states-condemns-russian-cyber-attack-against-the-country-of-georgia/. Accessed 11 May 2020; "The United States Concerned by Threat of Cyber Attack Against the Czech Republic's Healthcare Sector." Press Statement. *United States Department of State*, 17 Apr. 2020, https://www.state.gov/the-united-states-concerned-by-threat-of-cyber-attack-against-the-czech-republics-healthcare-sector/. Accessed 11 May 2020.

[19] While these recommendations were created prior to the National Cyber Strategy, they offer insight into what type of policies the State Department creates. Office of the Coordinator for Cyber Issues. "Recommendations to the President on Deterring Adversaries and Better Protecting the American People from Cyber Threats." *Office for the Coordinator for Cyber Issues*, United States Department of State, 31 May 2018, https://www.state.gov/wp-content/uploads/2019/04/Recommendations-to-the-President-on-Deterring-Adversaries-and-Better-Protecting-the-American-People-From-Cyber-Threats.pdf. Accessed 11 May 2020; Office of the Coordinator for Cyber Issues. "Recommendations to the President on Protecting American Cyber Interests through International Engagement." *Office for the Coordinator for Cyber Issues*, United States Department of State, 31 May 2018, https://www.state.gov/wp-content/uploads/2019/04/Recommendations-to-the-President-on-Protecting-American-Cyber-Interests-Through-International-Engagement.pdf. Accessed 11 May 2020.

[20] For more information on these type forums please see Peters, Allison and Amy Jordan. "Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime." *Journal of National Security Law and Policy*, 13 Feb. 2020, https://jnslp.com/wp-content/uploads/2020/02/Countering_the_Cyber_Enforcement_Gap.pdf. Accessed 11 May 2020.

[21] Marks, Joseph. "The Cybersecurity 202: U.S. to try new approach to punish hacking nations: Working with allies." *The Washington Post*, 7 Mar. 2019, https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/03/07/the-cybersecurity-202-u-s-to-try-new-approach-to-punish-hacking-nations-working-with-allies/5c80132b1b326b2d177d5ff1/. Accessed 11 May 2020.

[22] "Joint Statement on Advancing Responsible State Behavior in Cyberspace." Press Release, *United States Department of State*, 23 Sep. 2019, https://www.state.gov/joint-statement-on-advancing-responsible-state-behavior-in-cyberspace/. Accessed 11 May 2020; elarus, et al. "Countering the use of information and communications technologies for criminal purposes: draft resolution." *United Nations Digital Library*, United Nations, 2019, https://digitallibrary.un.org/record/3831879?ln=en. Accessed 11 May 2020.

[23] While this strategy was created prior to the National Cyber Strategy, it offers insight into what type of policies the State Department will create. United States Department of State, United States Agency for International Development. "Joint Strategic Plan FY 2018 - 2022." Feb 2018. https://www.state.gov/wp-content/uploads/2018/12/Joint-Strategic-Plan-FY-2018-2022.pdf. Accessed 11 May 2020.

[24] Lyngaas, Sean. "SamSam outbreak led to FBI restructuring, top official says." *CyberScoop*, Scoop News Group, 4 Apr, 2019, https://www.cyberscoop.com/samsam-investigation-fbi-tonya-ugoretz/. Accessed 11 May 2020.

[25] Lyngaas, Sean. "Inside the FBI's quiet 'ransomware summit'." *CyberScoop*, Scoop News Group, 6 Nov. 2019, https://www.cyberscoop.com/fbi-ransomware-summit/. Accessed 11 May 2019.

[26] Vavra, Shannon. "Secret Service to launch private-sector cybercrime council." *CyberScoop*, Scoop News Group, 22 Jan. 2020, https://www.cyberscoop.com/secret-service-private-sector-cybercrime-advisers/. Accessed 11 May 2020.

[27] "A Budget for America's Future Fiscal Year 2021." *Office of Management and Budget*, 2021, pp. 22, https://www.whitehouse.gov/wp-content/uploads/2020/02/budget_fy21.pdf. Accessed 11 May 2020.

[28] "U.S. Secret Service kicks off cyber incident response event in Atlanta." Press Release, *United States Department of Homeland Security, United States Secret Service*, 21 May 2019,

https://www.secretservice.gov/data/press/releases/2019/19-MAY/19_0521_USSS_dhs-atlanta-cyber-incident-response.pdf. Accessed 11 May 2020.