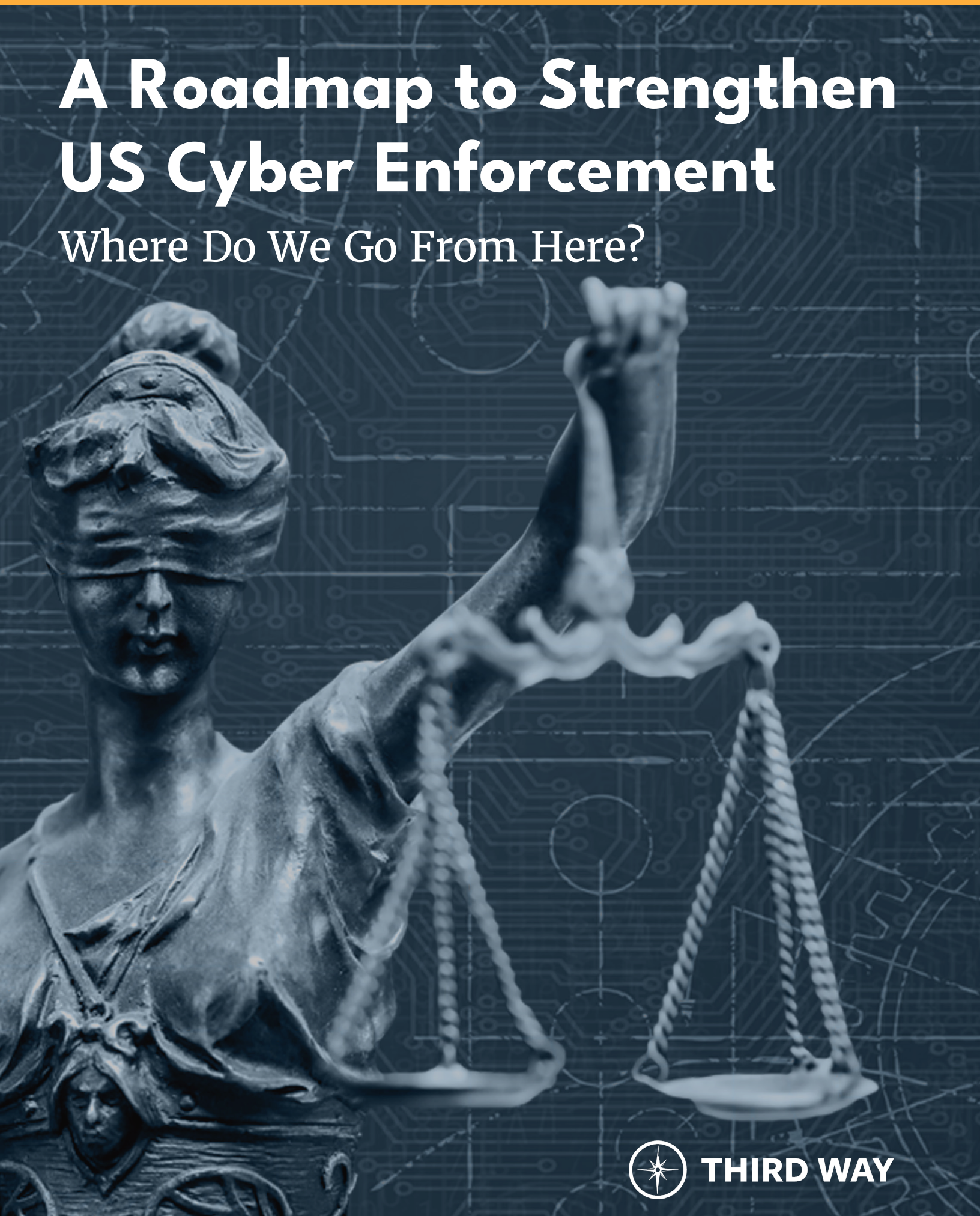
A Roadmap to Strengthen US Cyber Enforcement

Where Do We Go From Here?



THIRD WAY

Primary Author Biographies

Allison Peters, **Deputy Director of the National Security Program, Third Way**

Allison Peters is the Deputy Director of Third Way's National Security Program and Cyber Enforcement Initiative. She previously served as a consultant advisor to the United Nations and Organization for Security and Co-operation in Europe and was the Director of Policy and Security Programs at the nongovernmental organization Inclusive Security. Additionally, she spent many years serving in the US Senate, most recently as the senior foreign policy and national security advisor to the late Senator Frank R. Lautenberg (D-NJ).

Michael Garcia, **Senior Policy Advisor, Third Way**

Michael Garcia is the Senior Policy Advisor for Third Way's National Security Program and a Transatlantic Digital Debate Fellow for New America's Open Technology Institute and the Global Public Policy Institute. He is the former Director for External Engagement and Outreach for the US Cyberspace Solarium Commission and was a senior policy analyst for the Homeland Security Program at the National Governors Association.

THIRD WAY

November 9, 2020

Dear President-Elect Biden and Vice President-Elect Harris,

Congratulations on your victory! Now begins the hard work preparing our nation for the challenges of the future, and we look forward to working with you in combating the cyber threats our nation faces on a daily basis.

As part of that work, we are honored to present you with **"A Roadmap to Strengthen US Cyber Enforcement: Where Do We Go From Here?" This report is the result of a multiyear effort to define concrete steps to improve the government's ability to tackle the scourge of cybercrime by better identifying unlawful perpetrators and imposing meaningful consequences on them and those behind their actions.**

As Vice President-Elect Harris saw firsthand as California's Attorney General, cybercrime affects all sectors of our economy, from large corporations to local governments, hospitals, small businesses, and individuals. The FBI receives over 350,000 reports of cybercrime a year, with a dramatic rise during the COVID-19 pandemic. According to public polling, 1 in 4 American households is victimized by cybercrime, making it the most prevalent form of crime in the country. This cybercrime wave costs the US economy, by some estimates, over $100 billion annually. Sadly, our research finds that the number of arrests made in cybercrime cases is vanishingly small, relative to the threat—for every thousand reported incidents, only three see an arrest. This is a substantial cyber enforcement gap, and this is a crime for which perpetrators feel no consequence.

In this roadmap, we identify the challenges the US government faces in investigating and prosecuting these crimes and advancing the level of international cooperation necessary to do so. Cyberattackers take great pains to hide their identity, using sophisticated tools that require technical investigative and forensic expertise to attribute the attacks. The attacks are often done at scale, where perpetrators prey on multiple victims across many jurisdictions and countries, requiring coordination across criminal justice agencies. The skills necessary to investigate these crimes are in high demand in the private sector, making it difficult to retain qualified personnel. A number of diplomatic barriers make cross-border cooperation difficult, a challenge exacerbated often by blurred lines line between state and non-state actors in perpetrating these crimes.

While agencies work hard to respond, they lack coordination in doing so, creating confusion and ambiguity for both victims seeking justice and these agencies themselves. Law enforcement faces challenges collecting accurate data on cybercrime, hindering their ability to appropriately allocate resources and address shortfalls in technical expertise and investigative resources. International partners often lack the capacity or the will to address cybercrime emanating from their territory, and international frameworks and norms to address cybercrime are limited in the scope of countries that are represented. Further, a blame-the-victim attitude in cybercrime has often created tension in the relationship between the private sector and law enforcement, rather than on the common goal of catching the perpetrator(s).

These challenges are steep but not insurmountable. To address them, we assembled experts with expertise in law enforcement, diplomacy, and cybersecurity. We convened a working group on the White House led by Ari Schwartz, former special assistant to President Obama and senior director for cybersecurity, and Mary DeRosa, Deputy Assistant and Deputy Counsel to the President in the Obama Administration. On law enforcement challenges, we convened a working group led by former FBI General Counsel Jim Baker and Mieke Eoyang, Senior Vice President for Third Way's National Security Program. For global challenges, we convened a working group led by Chris Painter, former Coordinator for Cyber Issues at the State Department, Ambassador (ret.) Gina Abercrombie-Winstanley, and Allison Peters, Deputy Director of Third Way's National Security Program. In addition, Eileen Decker, former US Attorney for the Central District of California, and Jennifer Daskal, former counsel to the Assistant Attorney General for National Security at the Justice Department, led sub-groups focused on state and local law enforcement, and cross-border data sharing respectively.

This roadmap recommends actions that your administration can take to develop a comprehensive strategy to reduce cybercrime and minimize its impact on the American people by identifying the perpetrators and imposing meaningful consequences on them. We propose you make clear at the outset to the American public and global partners that cyber enforcement will be a top priority for your administration. In reinstating a White House cybersecurity position, we have extensive recommendations on how that position should address cybercrime. And, to make policy from an intelligence baseline, we believe you should request a National Intelligence Estimate on the linkages between cybercrime and nation-state cyber actors to understand the scope of the problem.

Our law enforcement working group has detailed recommendations to improve and modernize law enforcement's ability to track and respond to cybercrime. And our global cooperation working group has detailed recommendations on creating a cohesive international cyber engagement strategy; assessing and improving the capacity of foreign partners on cybercrime; and improving the process for cross-border data requests that are critical to solving these crimes. We believe that with these recommendations, you can make substantial strides in bringing cybercriminals to justice and deterring future cybercriminals from victimizing Americans.

We recognize that this report comes to you amid the urgent need to address systemic racism in policing that has undermined trust between law enforcement and the public. As you consider how to reallocate funds to address community needs and reform policing in our nation, we hope you will also modernize criminal justice responses to cybercrime. Our team stands ready to assist your administration and are confident that you will lead the nation and the world in addressing this ongoing threat.

Sincerely,

Mieke Eoyang,

Senior Vice President, Third Way National Security Program

RECOMMENDATIONS TIMELINE

The diagram below provides a timeline of when each recommendation in this report should be initiated and the US government entity responsible for its implementation:

Table of Contents

Acknowledgements

To develop the recommendations in this roadmap, Third Way's Cyber Enforcement Initiative convened three working groups of bipartisan, former high-level government officials, experts, and private sector representatives who provided their valuable expertise and experience on cybercrime and cyber enforcement. Each participated in their personal capacity, and their views do not reflect the positions of their institutions. We are grateful for the enormous amount of time they provided over several months to develop the ideas presented in this report.

The working groups focused on three thematic areas: The White House Cyber Enforcement Architecture, Law Enforcement Personnel and Capacity, and Global Cybercrime Cooperation. Co-chairs led each group in developing recommendations to address objectives that members identified as necessary no matter who occupies the White House in 2021. While all working group members reviewed the final set of objectives and recommendations, members largely provided contributions only to their working group.

Third Way would like to acknowledge and thank Mary DeRosa and Ari Schwartz, the co-chairs of the White House Cyber Enforcement Cooperation Working Group; Jim Baker and Mieke Eoyang, the co-chairs of the Law Enforcement Personnel and Capacity Working Group; and Ambassador (ret.) Gina Abercrombie-Winstanley, Chris Painter, and Allison Peters, co-chairs of the Global Cybercrime Cooperation Working Group. We also thank Eileen Decker for spearheading discussions on state and local cybercrime enforcement priorities and Jennifer Daskal for spearheading discussions on cross-border data sharing.

Third Way is grateful for the dedication and brilliant ideas contributed by all working group members:

White House Cyber Enforcement Cooperation	Law Enforcement Personnel and Capacity	Global Cybercrime Cooperation
Ari Schwartz (Co-Chair)	Mieke Eoyang (Co-Chair and Project Supervisor)	Gina Abercrombie-Winstanley (Co-Chair)
Mary DeRosa (Co-Chair)	Jim Baker (Co-Chair)	Chris Painter (Co-Chair)
Michael Daniel	Maggie Brunner	Allison Peters (Co-Chair and Primary Author of Global Recommendations)
Jordan Kelly	Eileen Decker	Shilpa Bratt
	Mike Donaghey	Scott Charney
	Jim Emerson	Kaja Ciglic
	Michael Garcia (Primary Author of Law Enforcement Recommendations)	Jennifer Daskal
	Kristin Judge	Jim Dempsey

	Matt LaVigna	Thomas Dukes
	Jeff Lybarger	Robyn Greene
	Jim McDonnell	Mark Iozzi
	Sunjeet Randhawa	David Lieber
	Eric Wenger	Tim Maurer
	Tyler Wotring	Adam Segal
		Stephen Tankel
		Andy Taylor
		Ian Wallace

Third Way also acknowledges and thanks the individuals who assisted behind the scenes with drafting and design, including Jim Kessler, Anisha Hindocha, Timothy McGiff, Micalyn Struble, Diana Sanchez, Kalyn Simmons, and Patrick Shilo. Additionally, we are grateful to the many experts and policymakers who provided us with feedback and input throughout the process.

Last but certainly not least, we thank the William and Flora Hewlett Foundation for its generous support for Part 1 of this report, The Case, which allowed us to explore and map the current challenges faced by the US government on cyber enforcement. The policy recommendations contained in Part 2 of this publication were exclusively funded by Third Way.

THIRD WAY

PART 1

The Case

The United States faces an unrelenting cybercrime wave that affects nearly every sector of the American economy and threatens US security. As more Americans rely on the Internet and the COVID-19 pandemic causes computer use patterns to change, opportunities grow for cybercrime perpetrators.[1] Much of America's debate about cybersecurity policy focuses on defending the country from cyberattacks. However, an existing and growing enforcement gap permits perpetrators of cybercrime targeting American people, companies, and governments to face little to no consequences for their actions. Public opinion research makes clear that American people want more aggressive action from US policymakers to combat cybercrime and punish the culprits. This will require a robust approach that strengthens tools for law enforcement and international diplomacy responses.

The start of a new presidential term in 2021 is an opportunity for the US government to take stock of the myriad challenges that have stymied progress in the global enforcement of cybercrime and to design a strategy to finally address them. In partnership with a bipartisan group of former high-level government officials, experts, and private sector representatives, Third Way launched a project to assess these challenges and propose a cyber enforcement roadmap for the presidential administration in 2021. **Our goal is to help the next presidential administration develop a comprehensive cyber enforcement strategy to reduce cybercrime and minimize its impact on the American people by identifying the perpetrators and imposing meaningful consequences on them.**

Part 1 of this paper provides an assessment of the current cybercrime problem and impediments to progress. Part 2 proposes a roadmap with detailed, actionable policy recommendations for a new and comprehensive approach to US cyber enforcement that the White House can launch in January 2021 and implement over the next two years.

America's cybercrime wave and persistent enforcement gap.

The United States is in the midst of a long cybercrime wave targeting America's people, governments, businesses, and organizations, with no end in sight. Ransomware (a form of cybercrime) has taken entire state and local governments offline, costing millions in recovery costs.[2] Senior citizens have lost millions of dollars to cybercriminals.[3] And nation-states are turning to cybercrime to steal America's closely guarded national security secrets and intellectual property (IP).[4]

The COVID-19 pandemic has exposed even more opportunities and vulnerabilities. In April, one month into the pandemic, the Federal Bureau of Investigation (FBI) saw an uptick in daily cybercrime reports of more than 400% compared to their typical complaint rates.[5] Two months later, a top US Secret Service (USSS) official estimated that cybercriminals would steal

and scam Americans out of $30 billion in stimulus funds.[6] Cybercriminals directly targeted the healthcare sector at a time when it faced unprecedented strain due to the pandemic, extorting hospitals and demanding ransom payments to unlock critical data that could keep people alive.[7] In one such case, the impact of a ransomware incident is suspected to have led to the death of a patient in Germany.[8] The World Health Organization also reported a five-fold increase of malicious cyber incidents since the outbreak of COVID-19.[9]

Even before the pandemic, one in four American households had been victimized by cybercrime, making it the most prevalent crime in the United States.[10] Key data points include:

- The financial impact of ransomware alone increased 1400% between 2015 to 2017.[11]
- Phishing emails grew over 40% between 2017 and 2018, and the healthcare sector saw a 473% increase of email fraud from 2016 to 2018.[12]
- A 2018 White House Council of Economic Advisors report estimated that malicious cyber activity cost the US economy anywhere from $57 billion to $109 billion in 2016, and that the price tag would continue to rise.[13]
- In the private sector, the professional services firm Accenture found that the average cost of cybercrime for companies increased by 12 percent between 2017 and 2018, from $11.7 million to a new high of $13 million.[14]

A wide range of actors have taken up cybercrime to advance their varied objectives, including state-sponsored or -enabled actors, organized criminal groups, and lone actors. Some US assessments indicate organized criminals and lone cybercriminals are generally motivated by financial reasons, while nation-state actors tend to be more focused on stealing, destroying, or compromising victim data.[15] The line between nation-state actors and non-state cybercriminals is blurring as states abet and directly employ non-state cybercriminals and/or their tools.[16] For example, in July 2020, the Department of Justice (DOJ) indicted two criminals contracted by the Chinese government to steal COVID-19 vaccine IP, who also hacked companies for personal financial gain.[17] This blurring line between state and non-state actors has complicated the ability of governments like the United States to identify the perpetrators of cybercrime and hold them fully accountable.

The current cyber enforcement gap in the United States means cybercriminals largely operate with impunity, rarely facing consequences for victimizing America's people and institutions.

The widespread use of technology and the growing rates of internet connectivity around the globe, coupled with the continued development of technologies that allow for anonymity on the Internet, have made cybercrime a low-risk, high-yield venture. Unfortunately, law enforcement in the United States and globally has struggled to keep pace. In the United States alone, Third Way found that only 3 in 1,000 cyber incidents reported to the FBI lead to an arrest.[18] The real gap between incidents and arrests is likely even higher, as victims often do not report

cybercrimes.[19] Available global data indicates that the enforcement gap is no better in many countries where the United States needs support to combat this transnational threat.[20]

The current cyber enforcement gap in the United States means cybercriminals largely operate with impunity, rarely facing consequences for victimizing America's people and institutions. The American people want this to change.

Americans want to see the cyber enforcement gap reduced.

An August 2019 poll of 1,685 likely US primary voters found that 92% of respondents said it was important for the next US President to make reducing cybercrime a top priority.[21] In a 2018 Statista poll, 72% of respondents worried that hackers would steal their personal, credit card, or financial information, placing this concern highest among a list of thirteen crimes.[22] Further, a 2019 Chicago Council on Global Affairs survey found that a majority of the 2,000 respondents polled rated cyberattacks on the United States as a top national security threat, mirroring findings in an April 2020 Pew Research Center poll.[23]

When it comes to bringing cybercriminals to justice, voters believe the federal government is the most important actor. According to a Third Way and Global Strategy Group survey conducted in early 2020 among 2,000 likely voters, 60% believe it is the federal government's responsibility to investigate and prosecute cybercrime.[24]

The presidential administration must prioritize reducing this gap in 2021, something that will require a mindset shift and a rebalance of US cybersecurity policies.

Solving the cyber enforcement gap requires a fundamental rebalance in US cybersecurity policies from a heavy focus on building better cyber defenses against intrusion to waging an equally aggressive effort to identify and punish the people behind cyberattacks. This will mean shifting from a cybersecurity approach that often blames the victims to one that puts catching hackers at the forefront.[25] An approach that emphasizes apprehending criminals and balances international diplomacy with other US capabilities in cyberspace would benefit both the American government and people.

There are many types of cybercriminals, and many types of cybercrimes. The response required by the US government will depend on the specific circumstances of each specific case. To date, however, the US government has over-emphasized and -resourced military responses to secure cyberspace from nation-state actors and impose consequences on them, while America's domestic law enforcement has not received the level of resources, training, and focus necessary to sufficiently identify, deter, and punish offenders, particularly non-state actors. Further, a militarized, national security approach provides little to no transparency for the American public to understand the country's own cyber operations, which are often hidden in classified programs.[26] Additionally, if other countries think a militarized response to malicious cyber activity is the acceptable norm and respond in kind, there is a risk of future military cyber escalation.[27] Finally, an approach that overemphasizes defensive, militarized action may inadvertently cause policymakers to overlook malicious cyberattacks for private, financial gain and instead focus largely on attacks against US critical infrastructure, despite billions lost annually to ubiquitous cybercrime.[28]

American policymakers must also change another held mindset if they want to tackle the enforcement gap: they must stop believing that an effort to attribute attacks and punish those responsible is futile. In the past, critics have argued that enforcement actions do not deter future cyberattacks, particularly when it comes to criminals and state-sponsored or -sanctioned actors in the hardest to reach places. Research shows, however, that indictments and prosecutions play an important role in demonstrating the US government's ability to identify perpetrators, signaling the government's desire to obtain justice for victims and providing a foundation for government actions to deter future attacks, such as sanctions and diplomatic engagement.[29] When indictments and prosecutions are deployed strategically, they can be a critical component of broader efforts to punish the perpetrators of cybercrime and reduce its impact on all Americans. A comprehensive approach to combating malicious cyber activity and blunting its consequences would prioritize enforcement actions as one, but not the only, tool in America's toolbox against this activity. Depending on the perpetrator and activity, the government's response can include sanctions, asset forfeiture, and diplomatic efforts, as well as military and intelligence options when appropriate and legal.

In sum, cybercrime cannot be combated solely by brute military force or defensive efforts. Instead, the White House in 2021 must provide America's law enforcement and diplomats with the resources, capabilities, and knowledge needed to identify, stop, and bring to justice perpetrators of cybercrime.

The reasons behind the cyber enforcement gap require dedicated attention.

No single entity is solely responsible for cyber enforcement or addressing the challenges it raises. Cybercrime is difficult to track. The criminals often reside outside of the United States—some in countries either unwilling or unable to cooperate with the US government. Cyber enforcement requires a multitude of partners working seamlessly together across multiple domestic and international jurisdictions. But difficult is not the same as impossible. Accepting futility is not an option. The cybercrime threat is too pervasive and important to lack a dedicated, comprehensive approach for combating it.

Third Way convened nearly 40 experts to identify several large-scale bureaucratic, operational, and (geo)political challenges the United States must address to boost this cyber enforcement. They identified the following challenges:

- First, **the White House lacks an empowered, senior cybersecurity advisor** who can effectively coordinate federal efforts, promote information sharing, identify and fill intelligence gaps, and create a comprehensive cybercrime strategy. Cybercrime intersects cybersecurity, law enforcement, national security, and foreign policy agendas and therefore requires the engagement of many diverse government entities with varying missions, resources, expertise, and legal authority. While the role of a cybersecurity advisor who acts as a principal advisor to the President and to coordinate federal efforts has existed since the Clinton Administration, it has fluctuated in importance and responsibility. The position was effectively eliminated in 2018.[30] This hampers the government's ability to coordinate across the numerous federal entities who play critical roles in combating cybercrime and responding to domestic and international policy

issues, such as data privacy, that could have unintended impacts on cyber enforcement.[31] Without high-level leadership communicating, coordinating, and deconflicting among these entities, federal cybercrime efforts become muddled.

The lack of a senior cybersecurity advisor also hinders the government's ability to draw upon numerous categories of information, data, and intelligence held by different agencies to create a comprehensive picture of the cybercrime threat that can inform strategies to combat it and blunt its impact. Private and public sector entities have access to a wealth of cybercrime information and intelligence that is shared with the federal government, but the government's ability to effectively disseminating it to the right entities in a timely manner is the exception rather than the rule. The federal government must formalize a clear and consistent information sharing throughput that improves the timeliness and relevance of information while also addressing legal, cultural, and technological issues. For instance, while national security officials have taken steps to make the Vulnerability Equity Process (VEP) more transparent—the process in which the US government decides to publicly disclose or restrict a vulnerability— a senior cybersecurity advisor is needed to instill greater public confidence and collaboration in the VEP.[32] And a senior cybersecurity advisor can also work with the Intelligence Community (IC) to advance further assessments on the nature of the cybercrime threat. For well-founded reasons related to protecting privacy and civil liberties, the IC's primary mission is internationally focused and often unaligned with domestic law enforcement priorities. This dynamic, however, often results in delays in actionable information reaching the public and private entities tasked with dealing with the threat of cybercrime. Better aligning and formalizing cooperation with the IC represents a considerable challenge for these entities and a senior cybersecurity advisor can help address these issues.

White House Cyber Architecture Throughout the Years

Clinton, 1998

Richard Clarke
National Coordinator for Security, Infrastructure Protection, and Counterterrorism

Bush, 2001-2003

Richard Clarke
Special Advisor for Cyber Security

Bush, 2003 to Feb. 2004

Paul Kurtz
Special Assistant to the President and Senior Director for Critical Infrastructure Protection on the White House's Homeland Security Council

Bush, Aug. 2005 to 2009

Marie O'Neill "Neill" Sciarrone
Special Assistant to the President for Cybersecurity and Information Sharing Policy

Obama, Feb. 2009 to Dec. 2009

Melissa Hathaway
Acting Senior Director for Cyberspace for the National Security and Homeland Security Councils

Obama, Dec. 2009 to May 2012

Howard Schmidt
Special Assistant to the President and Cybersecurity Coordinator on the National Security Council

Obama, June 2012 to Jan. 2017

Michael Daniel
Special Assistant to the President and Cybersecurity Coordinator on the National Security Council

Trump, March 2017 to May 2018

Rob Joyce
Cyber Coordinator

Trump, May 2018 to Present

Cyber coordinator role eliminated and demoted within the National Security Council and split between two positions

Sources:

"The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63," The White House, May 1998 https://clintonwhitehouse4.archives.gov/textonly/WH/EOP/NSC/html/documents/NSCDoc3.html Accessed 13 Oct 2020.

"New Counter-Terrorism and CyberSpace Security Positions Announced," The White House , 9 October 2001 https://georgewbush-whitehouse.archives.gov/news/releases/2001/10/20011009-4.html Accessed 13 Oct 2020.

The roles and responsibilities of this role were diminished following Richard Clarke's departure due to Executive Order 13286 abolishing Clarke's former position. "Off-the-Record Discussion with Paul Kurtz." Partnership for a Secure America, 9 February 2017. https://psaonline.org/paul-kurtz/ Accessed 13 Oct 2020.

"Personnel Announcement," The White House, 28 November 2007, https://georgewbush-whitehouse.archives.gov/news/releases/2007/11/20071128-9.html Accessed 13 Oct 2020.

"President Obama Directs the National Security and Homeland Security Advisors to Conduct Immediate Cyber Security Review," The White House, February 2009 https://obamawhitehouse.archives.gov/realitycheck/the-press-office/president-obama-directs-national-security-and-homeland-security-advisors-conduct-im Accessed 13 Oct 2020.

Phillips, Macon, "Introducing the New Cybersecurity Coordinator," The White House , 22 December 2009 https://obamawhitehouse.archives.gov/blog/2009/12/22/introducing-new-cybersecurity-coordinator Accessed 13 Oct 2020.

"Michael Daniel" Cyber Threat Alliance, https://www.cyberthreatalliance.org/biography/michael-daniel/ Accessed 13 Oct 2020.

Grant Schneider filled this position from July 2018 through July 2020. Joshua Steinman fills the other position. Geller, Eric. "White House Eliminates Top Cyber Adviser Post" Politico, 15 May 2015 https://www.politico.com/story/2018/05/15/white-house-eliminates-cyber-adviser-post-542916 Accessed 13 Oct 2020.

- Second, law enforcement cannot accurately measure the cyber enforcement gap and assess progress, because **the federal government lacks comprehensive data on how often cybercrime occurs.** Currently, fewer than one in ten victims of cybercrime report the crime to law enforcement, in part due to uncertainty about which agency to report to.[33] Victims may also see no utility in reporting a crime to law enforcement because they rarely receive updates on the status of their report and lack assistance dealing with the financial loss and mental health consequences stemming from the crime. Private sector companies, too, hesitate to report cybercrime to law enforcement due to potential regulatory consequences and loss in profits.[34] And when crimes are reported to federal and state, local, tribal, and territorial (SLTT) law enforcement, there are various federal databases that they could be entered into, but these databases are neither interoperable nor collected into a central repository.[35] As a result, the federal government lacks a comprehensive picture on how often cybercrime occurs. This causes policymakers to deprioritize it compared to other crimes and makes it impossible to establish useful metrics to reduce cybercrime or to provide resources commensurate with the threat.
- Third, **the federal government does not provide law enforcement personnel with the technical capabilities to analyze digital evidence or the training opportunities needed to expand and diversify the workforce.** Over half of local law enforcement agencies do not have access to the resources they need to process digital evidence, even though nearly every crime now produces some digital footprint.[36] These agencies rely heavily on federal crime labs to assist them in digital forensics, but these labs tend to be inaccessible to rural law enforcement agencies.[37] Compounding this challenge is the technical competencies SLTT criminal justice personnel need to perform digital forensics analysis to conduct cybercrime investigations.[38] Recruiting new individuals with these skill sets is exceedingly difficult, with nearly 3,000 public sector jobs for analysts and investigative positions going unfilled.[39] At the same time, programs to recruit and train federal and SLTT personnel on skills related to digital evidence forensics have been defunded or seen their funding levels remain stagnant despite the rise in cybercrime.[40] For example, the budget for the FBI's National Domestic Communications Assistance Center (NDCAC), which offers various technical and training assistance to SLTT on digital evidence, was projected to decrease by 25% with expected funding cuts over the past eight years while the FBI's total budget has increased roughly 16% during that same period.[41]

  Further, women, minorities, and other underrepresented groups are not adequately recruited, as Black and LatinX employees make up less than 20% of the FBI workforce and women make up only a third of the Department of Homeland Security's (DHS) workforce.[42] Research demonstrates that diverse workforces produce better outcomes and more informed decision-making.[43] Public agencies also struggle to retain trained employees who are lured away to the private sector to receive higher salaries.[44] Due to the skills and training gap, the 18,000 SLTT law enforcement agencies in the United States need more robust partnerships with the federal and private partners to make progress, while expanding diversity, equity, and inclusion initiatives. Addressing these training

and workforce gaps will likely require increased federal spending. However, the Government Accountability Office (GAO) reported this year that the White House lacked insight into how much agencies should be spending to implement the 2018 National Cyber Strategy, which includes cybercrime goals and commitments on training.[45]

- Fourth, **perpetrators of cybercrime are often located in countries unwilling or unable to cooperate with US diplomats and law enforcement in a timely manner.** The US international engagement architecture is not set up at the level needed, nor operated at the efficiency required, to overcome these challenges. A single cybercrime incident can hit victims in multiple countries independent of the location of the perpetrators, which means cybercrime investigations frequently involve criminal justice systems that may, in some cases, lack capacity, tools, and/or harmonized legal regimes. Extradition can be complicated and lengthy. While the US government has provided foreign assistance to governments and international organizations to build capacity on cybercrime, it has largely underinvested in these efforts in comparison to capacity building to combat other security threats. Further, the entirety of this foreign capacity building assistance is extremely difficult to track.[46] No mechanism exists to assess, monitor, and evaluate these security assistance efforts to determine whether they are achieving objectives and including adequate human rights safeguards to prevent against misuse. This is critically important, as many governments around the globe have used cyber enforcement tools and capabilities to perpetrate human rights abuses and undermine the rule of law.[47]

  For governments that are systematically unwilling to cooperate with the United States, the challenges vary widely depending on the nature of the nation-state and the motivations of the cybercriminal(s). Some governments have "passive" relationships with cybercriminals. They may criminalize such activity but are unable to stop attacks for many reasons, including corruption. In these cases, capacity building and other forms of direct support may be critical. However, some governments ignore or abet malicious cyber activity or directly order or execute attacks themselves, at times employing non-state cybercriminal proxies. Other diplomatic, law enforcement, economic, military, intelligence, or offensive cyber activities may be necessary to incentivize or compel a change in behavior.[48]

  The US government has prioritized the establishment and strengthening of norms guiding responsible state behavior in cyberspace to address the actions of America's adversaries. Yet the US government has not always been in lockstep with its allies in the development of such norms.[49] Advancing accountability and enforcement of cyber norms must continue to be a core objective of US cyber diplomacy. And for them to have widespread impact, the United States must be willing to abide by such norms—something it has not always been willing to do. The development of global cyber norms for nation-states must go hand-in-hand with efforts to identify, stop, and bring to justice cybercriminals. This includes the strong promotion of membership to the only legally binding global cybercrime treaty known as the Budapest Convention in order to facilitate cross-border cooperation in these cases.[50] These two priorities must be pursued in a

complementary and reinforcing manner, with the US government leveraging debates on global cyber norms to remind governments of their responsibilities to identify and prosecute cybercriminals.

Unfortunately, the US government currently lacks the robust international engagement architecture to overcome these global challenges. US efforts to impose consequences on countries for malicious cyber activity are hindered by a weakened American diplomatic corps.[51] The US government needs high-level cyber diplomacy leadership with the resources and personnel to support their efforts, including a US cyber ambassador position and office at the Department of State (DOS). Even with such an office, there will be challenges around deconflicting its role in relation to other government departments and agencies that engage internationally on these issues.

Additionally, America's retreat from the global stage and multilateral engagement will continue to hinder progress on cyber enforcement. Combating the cybercrime threat requires prioritization at the highest levels of the US government and the expert personnel and resources to advance global engagement—two things that have been inadequate under past administrations. Reasserting US leadership globally on cybercrime and cyber issues more broadly and strengthening multilateral engagement must be a top priority. It will be particularly critical as the presidential administration grapples with if and how the US government will engage in negotiations on a new global cybercrime treaty pushed by Russia. And it will be vital as the US government and other supporters of an open, free, and secure Internet engage in an ongoing global competition with governments who support a more authoritarian model of Internet control on debates around cybersecurity and technology policy more broadly.[52] The next administration will need to rebuild and reorient the US international engagement architecture to strengthen US global leadership on information and communication technologies (ICT) issues and promote a strong commitment to an open, free, and secure Internet.

- Fifth, and lastly, **the current mechanisms the US government uses to share and request cross-border data remain too slow and cumbersome to make substantial progress on cyber enforcement.** The US government needs robust partnerships with other countries and the private sector to help investigate, arrest, prosecute, and, when warranted, extradite cybercriminals operating outside US jurisdiction. But the burdensome process for foreign governments to request cross-border data sharing disincentivizes such cooperation and slows investigations. Attempts in recent years to overcome these challenges, including the passage of the Clarifying Lawful Overseas Use of Data (CLOUD) Act, may have an impact, but they will only be applicable to a limited number of governments.[53] Efforts by certain governments to force data to be stored locally will only serve to further restrict these cross-border data flows.

Reasserting US leadership globally on cybercrime and cyber issues more broadly and strengthening multilateral engagement must be a top priority.

A New Approach to Cyber Enforcement.

From April to October 2020, Third Way convened three bipartisan working groups of former high-level officials from Democratic and Republican administrations, state and local governments, private sector representatives, experts, and academics to create detailed, in-depth policy recommendations on cyber enforcement for the Administration in 2021. These consensus recommendations provide a roadmap toward a comprehensive cyber enforcement strategy that reduces cybercrime by increasing the rate at which global perpetrators are identified and brought to justice.

Some recommendations are for the first 100 days of the Administration; others concern new institutions, mechanisms, and assessments to be introduced within the first two years to achieve whole-scale government reforms.

The working groups were organized around three topics:

1. **White House cybercrime architecture**, with a focus on how the next Administration should unify cybercrime policy across the federal government, improve engagement with the private sector, and pave a strategic way forward for cyber enforcement efforts;

2. **Law enforcement personnel and capacity**, with a focus on how federal and SLTT criminal justice agencies can better receive, investigate, and respond to cybercrime, as well as arrest and prosecute criminals; and

3. **Global cybercrime cooperation**, with a focus on how the US government can better cooperate with and support foreign governments' efforts to impose consequences on perpetrators of cybercrime.

Part 2 of this paper establishes the following objectives for the presidential administration in 2021:

WHITE HOUSE CYBER ENFORCEMENT ARCHITECTURE

Objective 1: Create and empower a National Cyber Advisor position within the Executive Office of the President.[54]

Objective 2: Enable the Office of the National Cyber Advisor to coordinate with federal agencies to identify, resolve, and develop proposals to improve interagency processes and federal partnerships with external stakeholders to close the cyber enforcement gap.

Objective 3: Introduce legislation that permanently places the VEP under the purview of the Office of the National Cyber Advisor and increases the transparency of the VEP.

Objective 4: Update the US government's approach to cyber threat intelligence collection and sharing around cybercrime.

Objective 5: Develop a dedicated strategic approach to cyber enforcement as part of a US national cyber strategy.

LAW ENFORCEMENT PERSONNEL AND CAPACITY

Objective 6: Identify and clarify roles and responsibilities for cybercrime investigations among

federal and SLTT entities to strengthen institutionalized processes and relationships with public, private, and international partners.

Objective 7: Increase prioritization of cybercrime among federal, SLTT, and private sector stakeholders and direct federal resources to federal and SLTT agencies that are commensurate with its prevalence and impact.

Objective 8: Develop uniform metrics to inform and improve data reporting, victim response, and national data collection mechanisms for federal and SLTT law enforcement.

Objective 9: Strengthen federal and SLTT law enforcement's ability to share investigative information related to cybercrime.

Objective 10: Improve the digital evidence forensic capacity and capability of federal and SLTT criminal justice agencies by reforming recruitment, training, and retention practices.

Objective 11: Assess the needs, resources, and capacity of SLTT criminal justice agencies and federal–state collaborative organizations to address cybercrime.

GLOBAL CYBERCRIME COOPERATION

Objective 12: Establish a new DOS structure to ensure a well-resourced single point of high-level leadership for all cyber diplomacy matters, backed by an architecture that allows for other bureaus advancing policy and programming on cybercrime to effectively coordinate.

Objective 13: Identify a set of diplomatic tools and policy options to boost international cooperation in cybercrime investigations and address governments that are systematically uncooperative.

Objective 14: Identify a group of countries where the US government is not receiving timely assistance in cybercrime investigations and develop programs to support their criminal justice capacity building needs—including operational support, policy development, and harmonization of laws—to boost cooperation.

Objective 15: Streamline the process and improve the timeline for responding to cross-border data requests, in accordance with substantive and procedural protections.

MONITORING AND MEASURING IMPLEMENTATION

Objective 16: Establish processes at lead agencies to measure the implementation of all objectives.

While the objectives above have implications for US policy on a broad range of cyber-related issues, the recommendations to implement them are organized around a unified goal: imposing consequences on the perpetrators of cybercrime and providing justice to their victims in order to reduce the damage cybercrime is causing in America. Americans of all stripes are being victimized daily by cybercrime, and US policymakers must take decisive action to answer this threat. Jurisdictional and geopolitical challenges, insufficient resources, and a lack of an organized government architecture can no longer justify a US cybersecurity strategy that fails to prioritize cyber enforcement. It is critical that the United States have its own cyber enforcement house in order as it competes on the global stage with countries like China and Russia on issues and standards around cybersecurity and technology policy more broadly. It is time for the United States to close the cyber enforcement gap.

THIRD WAY

PART 2

The Roadmap

Presidential administrations have undertaken important efforts to bring perpetrators of cybercrime to justice. But the rising cybercrime wave and yawning cyber enforcement gap makes clear that these are not enough. Today, cybercriminals largely operate with impunity. And the people working on these issues day and night need, and deserve, more support from the highest levels of the US government. Change must start with a presidential administration in 2021 that puts cybercrime at the forefront of America's cybersecurity agenda and commits the US government to a new, comprehensive approach to cyber enforcement.

The policy recommendations below are from the three bipartisan working groups Third Way convened to develop a roadmap on cyber enforcement. Some actions are for the first 100 days of a presidential administration; others will take longer. Many will affect a wide range of cyber-related challenges the US government is facing.

Recommendations are grouped around three themes: The White House Cyber Enforcement Architecture, Law Enforcement Personnel and Capacity, and Global Cybercrime Cooperation. Many recommendations are complementary and, at times, contingent upon each other. Implementation timelines are noted in parenthesis after each.[55] The working groups tried to identify and prioritize those recommendations that make structural changes within the US government and that create assessments needed to inform and implement policies and strategies for cyber enforcement in the longer term.

White House Cyber Enforcement Architecture

Objective 1: Create and empower a National Cyber Advisor (NCA) position within the Executive Office of the President (EOP).

1.1 The NCA should be located within the EOP (Day 0).

With the 2018 removal of the White House Cybersecurity Coordinator, the President lacks a principal, senior staff advisor on cyber policy. This removal signaled to many that the United States deprioritized cybersecurity. It must be reversed. The NCA should be located within the EOP to advise the President directly. The President should install the NCA as their principal advisor and coordinator on cyber issues and ensure that the position is staffed and empowered to perform this role effectively. The NCA should be a staff position with a role similar to that of the National Security Advisor, Homeland Security Advisor, and National Economic Advisor. The President should create this position as part of their presidential directive to establish the administration's National Security Council (NSC).

Once appointed, the NCA should work across agencies to develop a domestic and international engagement plan on cybercrime. This should include identifying opportunities to demonstrate presidential-level commitment to this issue globally, such as making it a component of the President's speech at the United Nations (UN) General Assembly or during the 10-year anniversary of the opening of the Budapest Convention in November 2021.

1.2 The NCA should be an NSC deputy (Day 0).

Because cyber issues are critical and intersect with other NSC constituents, the NCA should serve on the NSC Deputies Committee. The NCA should be invited to all NSC meetings that address cybersecurity, and NSC staff should be involved when NCA efforts affect national security. The National Security Advisor, the NCA, and their staffs should collaborate closely on cybersecurity matters and maintain frequent, open communication.

1.3 The NCA should not require Senate confirmation (Day 0).

The NCA would best fulfill their cybersecurity responsibilities as a presidential advisor integrated into the NSC staff, so the position should not be subject to Senate confirmation. Other similarly situated presidential advisors are not Senate confirmed, because to do so would interfere with the President's ability to choose and interact with their closest staff advisors. Like other senior presidential advisors, the principal roles of the NCA are to advise the President and develop and coordinate policy. Unlike Senate-confirmed officers, the NCA would not have operational authorities. A requirement of Senate confirmation—and the significant obligations for congressional testimony that come with it—would unnecessarily create distance from the President and undermine the trust and responsiveness that makes similar advisor roles so effective. Simply put, Senate confirmation of the NCA would diminish the President's ability to rely on the position.

1.4 The NCA should be supported by an Office of the National Cyber Advisor (ONCA) (Day 0).

The NCA should have the assistance of a well-staffed Office of the National Cyber Advisor (ONCA). Currently, no single office coordinates the overlapping responsibilities of federal agencies with cybersecurity responsibilities. The NCA needs staff to help manage the vast cyber policy development, coordination, and advisory process. In addition, the office will work with the many federal agencies with cybersecurity responsibilities to resolve conflicting priorities, develop policies and priorities, and provide leadership in resolving disputes between the government and the private sector around cyber policy.[56] The ONCA should be located outside the NSC because many of its responsibilities do not involve national security and will require frequent interaction with the private sector, which can be difficult inside the NSC.

1.5 The ONCA should play a role in planning, organizing, and overseeing strategic disruption of criminal infrastructure (Day 0).

Cybercrime disruption operations have policy implications and potential sensitivities around the actors involved, both of which require the type of central coordination that the ONCA can provide. Such a role is critical for overseeing strategic disruptions that fracture criminal relationships and ecosystems. The ONCA should help coordinate cyber operations that are both proactive and responsive. The NCA should orchestrate this coordination by using the NSC interagency process to prioritize and set the parameters for disruption operations and determine the broad, strategic rules of engagement for systemic disruption campaign activities.

To be clear, the NCA should have no operational authority; rather, the NCA should strictly coordinate and advise on policy. Neither the NCA nor ONCA should direct operations, and operational authority should remain with the agencies currently mandated to carry out such operations so as not to impede established processes or create jurisdictional conflict.

1.6 The ONCA should be allotted a staff of 25-30 people (Day 0).

With specific guidance for each role, 25-30 people would efficiently execute the responsibilities of the ONCA and would allow the Office to maintain effectiveness.[57] Staffing should center around specific policy challenges as well as the areas of threat response, asset response, and intelligence support as detailed in Presidential Priority Directive 41.[58] A staff of this size would not have the capacity to develop an independent policy process, so the ONCA should be encouraged to participate in pre-existing interagency policy processes and focus its efforts on advising interagency coordination. This recommendation would quintuple the current NSC cyber staff and would double the highest count of people dedicated to supporting the White House Cybersecurity Coordinator during the Obama Administration.

Staff should largely be composed of employees on rotating details, including details from DOJ and DHS to cover cybercrime issues. These positions should be staffed by personnel from the FBI and USSS. The ONCA should also hire a small number of permanent staff to support the office and maintain institutional knowledge.

This office should also share staff with the NSC, Office of Management and Budget (OMB), National Economic Council (NEC), and the Office of Science and Technology Policy. The former Office of the Cyber Coordinator was most effective when it harmonized its activities with other EOP elements. The US cyber community needs the NCA to provide leadership for the resolution of interagency disputes around cyber issues. Because the ONCA will need an in-depth understanding of the economic incentives involved in cybercrime, a member of the NEC should serve as a deputy in the ONCA.[59] This role should focus on tackling financial cybercrime and protecting the global financial system from abuse, as outlined in the updated National Cyber Strategy and in line with the recommendations of the 'International Strategy to Better Protect the Global Financial System Against Cyber Threats (2021-2024)' developed by the Carnegie Endowment for International Peace in partnership with the World Economic Forum.[60] As US cybersecurity priorities shift, the number of staff from each of these organizations may vary. To maintain agility, the ONCA should augment its staff with experts from academia, nonprofits, and SLTT governments through the Intergovernmental Personnel Act.[61]

1.7 The ONCA should have dedicated funding within the EOP budget (Day 0).

The EOP budget should include dedicated funding for the ONCA because an organization of this size must have its own congressional budget approval to work within the EOP. The White House should take a phased approach for funding this Office. For FY 2021, the ONCA should be funded through the White House. The FY 2022 budget should include a separate line item for the Office within the broader EOP budget and should give the ONCA the funding and authority to reimburse agencies for services, personnel, and facilities. The ONCA should also have the authority to hire private sector expertise on an expedited basis (such as through the US Digital Service), and to employ consultants and experts on a per diem basis. The ONCA is expected to cost between $5 million to $6 million annually.

1.8 The ONCA should concurrently review federal cybersecurity budgets with OMB (Day 0).

Part of fulfilling the coordination role for federal cybersecurity includes ensuring that proposed agency budgets are aligned with the administration's cybersecurity strategy. To do this, federal cybersecurity agencies should submit their budgets to OMB and the ONCA simultaneously. The ONCA should review the proposed agency budgets for consistency with the administration's cybersecurity strategy. Additionally, the Office should provide its analysis to both OMB and the submitting agency on where spending could be increased or decreased to align with the strategy. When OMB receives reprogramming transfer requests that affect cybersecurity funding, OMB should consult with ONCA. The ONCA should have at least one OMB staffer and one other person who interfaces with the OMB and budget staffers in other offices.

1.9 The ONCA should be transparent about its interaction with the private sector (Day 0).

Given the significant role that the private sector plays in cybersecurity, the ONCA should have the authority and responsibility to meet with representatives from the private sector. Non-NSC members of the ONCA staff should interface with the private sector. As an NSC deputy, the NCA would not meet directly with members of the private sector. In its work with the private sector, the ONCA should look to and support the recommendations and principles of initiatives focused on building public-private partnerships on cybercrime and cybersecurity, including the Carnegie Endowment's 'International Strategy to Better Protect the Global Financial System Against Cyber Threats (2021-2024)' and the World Economic Forum's Partnership against Cybercrime.[62] To further avoid the appearance of improper influence, the ONCA should maintain a clear, public record of staff meetings and their participants.

1.10 The ONCA should prioritize transparency by publishing an annual report (Day 0).

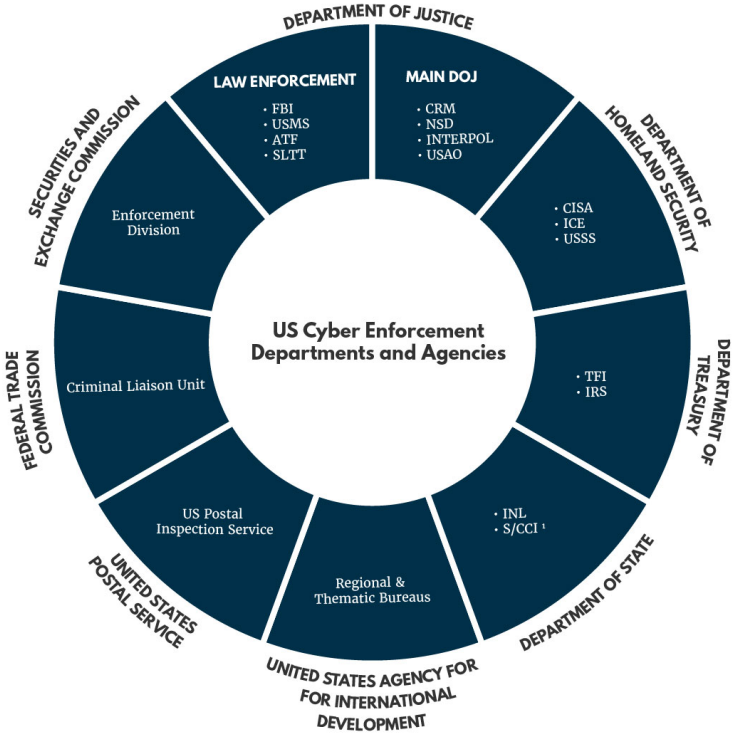
The ONCA should produce a yearly report for Congress and the public to foster accountability and public trust. In this report, the ONCA should publish a list of all meeting attendees to track interactions between the private sector and the ONCA, as mentioned above.[63] This report should also include the unclassified report on the VEP, which will be discussed in the following set of recommendations.

Objective 2: Enable the ONCA to coordinate with federal agencies to identify, resolve, and develop proposals to improve interagency processes and federal partnerships with external stakeholders to close the cyber enforcement gap.

2.1 The ONCA should lead a temporary, intergovernmental Cybercrime Working Group that consists of relevant federal entities to assess and develop interagency cyber enforcement policies and legislative proposals where cross-agency coordination and cooperation is required and to coordinate with the private sector and SLTT partners when necessary (0-100 Days).

Several federal entities have cybercrime missions that overlap, which requires ongoing coordination and cooperation across these entities to resolve legal, strategic, budgetary, and policy disputes and challenges. The National Cyber Investigative Joint Task Force (NCIJTF) coordinates interagency operational efforts related to cyber investigations, but no similar body exists to resolve policy disagreements on cyber enforcement, like how to best engage international partners, improve information sharing, and increase incident reporting.

THIRD WAY



LEGEND

- ATF: Bureau of Alcohol, Tobacco, Firearms and Explosives
- CISA: Cybersecurity and Infrastructure Security Agency
- 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
- 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.

This chart was updated in March 2020 using the information from the previous chart in the Reader's Guide to Understanding the US Cyber Enforcement Architecture and Budget from February 21, 2019.

The ONCA should lead a temporary, interagency working group (hereafter referred to as "The Cybercrime Working Group") that consists of the DOJ, DHS, DOS, FBI, the Department of Treasury, USSS, and other relevant departments and agencies to fill this gap. This would be a forum for developing policies and legislative proposals and resolving disputes on cybercrime policy where interagency coordination and consultation is particularly required.[64] This working group should be the forum for implementing the following recommendations where interagency policy coordination is required, among other priorities:

- Enhancing effective intergovernmental and public information sharing about cyber threat vectors (Recommendation 4.4).
- Clearly delineating cyber enforcement roles and responsibilities within federal entities and between federal and state entities to create more effective interagency coordination mechanisms (Recommendation 6.1).
- Developing proposals that improve cybercrime reporting among public and private victims and the assistance awarded to them (Recommendation 8.3).

- Enhancing information sharing mechanisms to improve investigative coordination (Recommendation 9.1).

Once the Cybercrime Working Group fulfills these recommendations, the ONCA should consult with the Working Group's members to determine if it should be dissolved or remain a standing forum to handle interagency policy disputes.

Objective 3: Introduce legislation that permanently places the VEP under the purview of the ONCA and increases the transparency of the VEP.

3.1 The NCA should work with Congress to develop legislation establishing a permanent Equities Review Board (ERB) within the ONCA (0–100 Days).

The VEP is the process by which the federal government "balances whether to disclose vulnerability information to the vendor with the expectation that they will patch the vulnerability, or temporarily restrict knowledge of the vulnerability so that it can be used for national security or law enforcement purposes."[65] The VEP Charter describes the vulnerabilities equities policy and process and provides guidelines for the VEP, including the composition and role of the interagency ERB.[66] The ERB is the primary forum for interagency deliberation and determination concerning the VEP.[67] However, despite the importance of having such an interagency forum to make these difficult decisions, the ERB is not legislatively mandated. To remedy this and ensure proper oversight, the NCA should work with Congress to develop legislation creating a permanent ERB within the ONCA.

Permanent members of the ERB should include representatives from the organizations in its charter.[68] The legislation should enable the NCA to add other permanent members or invite other agencies to attend meetings as needed.

3.2 In this legislation, Congress should establish a permanent VEP Director position to lead the ERB, supported by an Executive Secretariat (0–100 Days).

The VEP Director's responsibilities should be transferred from the NSC to a permanent position in the ONCA, which would now have the staff to support the VEP. While the NCA may elect to appoint someone to this position, the NCA could also choose to serve as the VEP Director. The Executive Secretariat, currently staffed by the National Security Agency, should be moved permanently to the ONCA.[69] This group would retain all responsibilities previously established through the VEP Charter.

3.3 Congress should require all US government agencies to timely submit all known vulnerabilities for review by the ERB (0–100 Days).

Currently, agencies share vulnerabilities with the ERB voluntarily. By requiring agencies to share all known vulnerabilities, the VEP would maximize its ability to protect Americans by giving the government time to get ahead of cyberattacks. This legislation should encourage the NCA and VEP Director (if the NCA chooses a separate person to serve as VEP Director) to collaboratively agree on a deadline by which agencies must submit vulnerabilities upon learning of them.

3.4 Congress should require the VEP Executive Secretariat to publish an annual report about the ERB (0-100 Days).

The VEP Charter from 2017 suggests, but doesn't require, that the VEP Executive Secretariat publish an annual report about the ERB.[70] The ERB has never done so.[71] This lack of transparency promotes skepticism about the process and sows distrust in the VEP's motives and efficacy. To reverse this trend, the legislation should mandate that the Executive Secretariat publish an annual report.

The report should include an unclassified section, delivered to Congress and published on the NCA's website, and a classified annex delivered only to the congressional intelligence committees. The unclassified section should contain aggregate information and metrics about the disclosure of vulnerabilities to give the public insight into the VEP and track its long-term effectiveness. This section may include the percentage of vulnerabilities disclosed to operators and manufacturers or the average time from discovery to the determination to disclose vulnerabilities.

The classified annex should include information about the types of vulnerabilities that were found and how they were used. It should identify which specific exploits from individual companies and platforms were disclosed and which were retained. This report should additionally identify which agencies most frequently called for vulnerabilities to be retained. Finally, this report should identify how many vulnerabilities are retained for espionage or law enforcement purposes, and how many vulnerabilities are retained for domestic or international criminal cases.

3.5 The VEP Director should clarify that the VEP applies to both purchased and internally discovered vulnerabilities (0-100 Days).

While the VEP has consistently been used to analyze vulnerabilities discovered by government agencies, it has been less clear on whether this process can be used for vulnerabilities purchased by the government. The VEP Director should publish a statement saying that the VEP will also be used to analyze purchased vulnerabilities. Eliminating gray areas to better define the parameters of the VEP ensures smoother operation and eliminates a source of contention between VEP stakeholders.

3.6 The VEP Director should ensure that voting power within the ERB is distributed equitably and should clarify the process to resolve disagreements (0-100 Days).

The legitimacy and efficacy of the VEP process rests on the notion that all perspectives are considered, and that voting power is fairly apportioned. Ideally, the ERB should try to achieve consensus with every decision to disclose or retain a vulnerability, and voting should be used only when consensus cannot be reached.

However, given the variability of the decision-making process of the VEP across administrations, the VEP Director should examine past votes to analyze and restructure voting within the ERB so that all the right voices are at the table. ERB voting rights should be granted solely to department-level agencies. Each department should have a single voting representative, but that representative may come from a sub-agency within the department. This representative should consult with the relevant sub-agencies before each ERB meeting to collect the agencies' input about each vulnerability.

The VEP Director should also clarify the decision-making process to disclose vulnerabilities when consensus cannot be reached and voting remains divided. A standardized process can streamline the length of time required to reach a conclusion by setting expectations, providing consistency, and allowing for precedent in decision-making. If no consensus can be reached and voting does not resolve disagreements, the decision to disclose or retain a given vulnerability should be sent to the NCA to call an NSC Deputies Committee meeting. The VEP Director should encourage subject matter experts to attend these meetings to explain the technical nature of cyber vulnerabilities.

3.7 The VEP Director should establish procedures for conducting regular reviews of the ERB (0–100 Days).

The VEP is a relatively new process that addresses a dynamic problem, so the current implementation must be monitored for inefficiencies and gaps. As such, the VEP Director should require the Executive Secretariat to conduct regular internal reviews of the VEP to answer the following questions:

- How often does each agency vote to disclose vulnerabilities?
- How many vulnerabilities has each agency recently submitted?
- What is the average length of the review process?
- Which parts of the review process are taking the longest amount of time?
- How often does the ERB have to ask for additional information before making a decision?
- Where do information gaps most frequently occur?

The VEP Director should also conduct regular reviews with VEP counterparts in other governments to determine which VEP models are the most efficient and effective.

Objective 4: Update the US government's approach to cyber threat intelligence collection and sharing around cybercrime.

4.1 ODNI and ONCA should create a joint working group to identify intelligence collection gaps on cybercrime and propose ways to close those gaps (0–100 Days).

The IC cyber collection capabilities are enormous, and they appropriately focus them on nation-state actors and the growing threat they pose.[72] On the other hand, private sector cybersecurity companies collect vast amounts of information on cybercrime, but that information is not always shared with the government. Even if private sector information were shared more systematically, that information alone is likely insufficient to support US government actions, such as arrest and prosecution. Therefore, the White House should establish a joint ODNI and ONCA working group to identify the intelligence gaps related to cybercrime and what sources could be used to fill those gaps. Where possible, the US government should seek private sector, non-profit, and foreign government sources for technical and contextual information, focusing IC assets on the key step of attribution to specific individuals.

4.2 The ONCA should integrate functional intelligence collection priorities related to cybercrime into regional intelligence priorities (101-180 Days).

The National Intelligence Strategy's topical mission objective of cyber threat intelligence should be better integrated into regional intelligence priorities.[73] Currently, intelligence resources are primarily aligned against traditional and legacy threats, and they typically do not prioritize or integrate information with cybercrime implications. All intelligence collectors should be trained to identify information that could potentially be related to the broad spectrum of cyber threats, not only high-end nation-states. Analysts looking at trends for specific countries or regions should be trained in cybersecurity terminology so that they can best search for cyber threat vectors. Within the first 100 days, the ONCA should create and disperse a cyber training guide for collectors and analysts covering different regional intelligence priorities.

4.3 The ONCA should work with the IC to update US government cyber threat intelligence analysis to produce adversary playbooks that describe cyber threat actors' typical tactics, techniques, and procedures (TTPs) (Day 0).

Consistent with the Department of Defense's "defend forward" approach, intelligence analysts should develop methods to predict where cybercriminals might move next and how their TTPs might evolve.[74] Taken as a whole, cyber incidents offer valuable insights into threat actors' operations and TTPs. The US government could use this information to develop "adversary playbooks," which would describe how different actor groups operate, map their operational steps, and catalog their TTPs. These playbooks would inform network defenders' priorities and guide the detection of additional malicious activity. Such playbooks could also identify where adversaries would be most vulnerable to long-term disruption and how their TTPs might evolve. The next Administration should encourage the IC to examine how rapidly evolving situations like global pandemics or social movements may shift TTPs. Organizations such as MITRE and companies like Palo Alto Networks are developing adversary playbooks based on private sector information; the IC should augment these playbooks with US government information.[75]

4.4 The Cybercrime Working Group should enhance effective intergovernmental and public information sharing about cyber threat vectors, including those related to cybercrime (0-100 Days).

Existing mechanisms for the distribution of cyber threat information from the government, like DHS Automated Indicator Sharing, are ineffective because they often provide the wrong information to the wrong constituencies.[76] This problem may partially stem from the burden on individual, resource-strapped organizations to identify what information to share with outside parties.[77] Therefore, the US government needs to refine its approach to information sharing and determine which organizations need to receive which type of cyber information. For example, most companies do not need and cannot use technical cyber threat information; instead, they need to know what concrete steps they should take to stop a new type of threat. The Cybercrime Working Group could help by identifying the types of cyber information that would benefit organizations, mechanisms for distributing that information, and opportunities to further declassify information to reach a wider audience. The Working Group should consult with the private sector, non-profit organizations, and related entities to develop this guide for effective information sharing activities.

As part of this effort, the Working Group should also review individual agencies' public information sharing alerts. Currently, each federal agency is incentivized to release public alerts about cyber threats and vulnerabilities to bolster the agency's reach and legitimacy.[78] However, this disaggregated communication often threatens other agencies' operations and appears disjointed. It disincentivizes members of the public from sharing cyber-threat information with the government because it is unclear which agency should receive information. In fact, DOJ lists eight different entities that span several DOJ and DHS agencies for victims and entities to report to.[79] The Working Group should develop a proposal to create a mechanism for the public to submit cyber threat information and allow for the distribution of this information to all necessary federal agencies. This proposal should require the ONCA to develop an interagency process to coordinate the publication and analysis of any cyber threat information shared with the public, as well as breaking down barriers that impede interagency information sharing.[80]

The ONCA should strive to incentivize robust participation in the Working Group. The willingness of government entities to share information is crucial to fostering stronger relationships with the private sector, which owns upwards of 85% of all critical infrastructure in the United States.[81] Only with agencies' willingness to fully participate can the federal government work best with the private sector to defend our nation's critical infrastructure from cybercrime.

4.5 The Director of National Intelligence (DNI) shall prepare a National Intelligence Estimate (NIE) on the relationship between criminal cyber actors and nation-states (Day 0).

Intelligence services of nation-state actors have relied on non-state, criminal actors to acquire and disseminate information, exploits, and funding. For example, in 2016 the Russian GRU, their military intelligence agency, developed a relationship with and relied upon non-state actors like Wikileaks to disseminate emails stolen from the Democratic National Committee and other individuals associated with a US presidential campaign.[82] As reported to the UN Security Council, North Korea has long pursued efforts to steal money from financial institutions and cryptocurrency exchanges to evade sanctions and has done so in cooperation with cybercriminals, including in Eastern Europe.[83] Criminals who steal massive databases with personally identifiable information may mine it for financial gain, while nation-state actors mine the same information for phishing attempts against high-value targets.

Intelligence services of nation-state actors have relied on non-state, criminal actors to acquire and disseminate information, exploits, and funding.

This NIE should review the capabilities, scope, activities, and impact of criminal cyber actors to better understand the evolving ecosystem of malicious cyber actors and their relationship to nation-state adversaries. The report shall include the community's estimate of the number of criminal organizations operating in cyberspace, their geographic distribution, and their relationship to nation-state governments. The DNI shall concurrently release an unclassified version of the NIE.

By identifying the tactics, relationships, and even identities of cybercriminals, the US government can develop an effective strategy to disrupt the ecosystem that feeds malicious cyber activity at the source.[84]

Objective 5: Develop a dedicated strategic approach to cyber enforcement as part of a US national cyber strategy.

5.1 The NCA should target a specific amount by which to reduce the economic impact of cybercrime by 2024 (101–180 Days).

Ultimately, the success of the NCA and the ONCA in tackling cybercrime will be determined by metrics of measurable impact (see Recommendation 8.1). First and foremost, the NCA should set a goal to reduce the impact of cybercrime on the US economy by a certain percentage by 2024. This number should be both ambitious and attainable. The NCA should select a point person within the ONCA to lead the development of a written strategy (see Recommendation 5.3) to achieve this goal. This person will ensure that the strategy is written by an established deadline and will lead all meetings related to its development.

5.2 ONCA staff should consult the private sector and civil society groups to identify barriers to the reduction of the economic impact of cybercrime (101–180 Days).

The private sector and non-governmental organizations are best positioned to identify the current policy, legislative, and diplomatic barriers to the reduction of the economic impact of cybercrime. The ONCA should meet with information sharing and analysis centers (ISACs) and sector coordinating councils (SCCs) to develop strategies to overcome these barriers.

5.3 The NCA should work through an interagency process to immediately draft a cybercrime addendum to the 2018 National Cyber Strategy and eventually strengthen the cybercrime components of a new or updated national cyber strategy (101–180 Days).

The NCA should work through an interagency process to update or draft a new national cyber strategy, which should occur every four years. This requirement will ensure that each administration strategically adapts to the ever-changing cyber landscape. By updating, instead of drafting a whole new strategy, the NCA can avoid spending time on an extended process, because most elements of the last strategy can and should remain consistent over time.

The 2018 National Cyber Strategy articulates four pillars to promote US cybersecurity, including one objective focused on cybercrime. This graphic details the priority actions of this cybercrime objective and the actors responsible for implementation.

However, due to the time and resources that it will take to develop a national strategy, the NCA should immediately work to draft a public addendum that details how the government will combat the threat of cybercrime to the 2018 National Cyber Strategy in the interim. Pillar 1 of the 2018 National Cyber Strategy aims to "Combat Cybercrime and Improve Incident Reporting," but is overly broad in how it would achieve objectives, misses critical components of a comprehensive cyber enforcement approach (as outlined in this roadmap), and lacks metrics to evaluate efforts to combat cybercrime.[85] After consulting with state and private partners through ISACs and SCCs, the ONCA should hold a meeting with representatives from federal agencies with cybercrime responsibilities to analyze the most significant barriers to reducing the economic and national security impacts of cybercrime and identify and implement concrete steps to overcome those barriers (see Recommendations 5.1 and 5.2).

Law Enforcement Personnel and Capacity

Objective 6: Identify and clarify roles and responsibilities for cybercrime investigations among federal and SLTT entities to strengthen institutionalized processes and relationships with public, private, and international partners.

6.1 The Cybercrime Working Group should clearly delineate cyber enforcement roles and responsibilities within federal entities, and between federal and SLTT, private, and international partners, to create more effective interagency coordination (101–180 Days).

At least 20 federal departments and agencies have key roles and responsibilities—which often overlap—in investigating, pursuing, and prosecuting cybercriminals.[86] Federal policies and laws describe components of these roles and responsibilities, but they do not delineate how these departments and agencies should interact with each other and coordinate where their jurisdictions overlap.[87] For example, DOS leads much of the US government's diplomatic engagement on cyber issues, but DOJ and other departments and agencies also develop US global cyber policy and work with foreign partners. Clarified roles and responsibilities in international cyber engagement is just one area where streamlined interagency coordination is required.

More clarity is also needed on federal entities' roles and responsibilities for coordinating with SLTT and private sector partners. SLTT criminal justice agencies have long partnered with federal agencies on traditional criminal cases, but these partnerships will need to adjust to account for the unique challenges associated with cybercrime. By contrast, the federal government does not have the same historical, routine partnerships with the private sector. With perpetrators of cybercrime abusing private networks and ICT infrastructure, federal law enforcement must develop a framework for when and how they partner with private companies to engage in disruption operations that target criminal infrastructure. While agencies have engaged in disruption operations with companies in the past, such as disrupting domains associated with COVID-19 scams, providing policy and legal clarity on such operations could further strengthen public-private partnerships.[88]

The Cybercrime Working Group (see Recommendation 2.1) should identify existing cyber enforcement roles and responsibilities within federal entities to improve and, when needed, create new interagency coordination mechanisms. Specifically, the Working Group should:

- Outline current federal departments and agencies' roles, responsibilities, and legal authorities and their associated challenges for receiving, responding, and investigating cybercrimes. This should also include challenges associated with arresting and prosecuting criminals and working with SLTT, foreign, and private partners in pursuing these efforts.[89] The Working Group should then develop policy and legislative proposals that address these challenges.
- Conduct cost/benefit analyses of previous administration and congressional proposals to reform the US cyber enforcement architecture, such as moving the USSS back to the Treasury Department.[90] This analysis should also consider possible organizational reforms within DOJ to help cybercrime investigations and

prosecutions become more efficient, nimble, standardized, and better coordinated within the Department and across its US Attorney Offices.

- Review, clarify, and/or create appropriate thresholds (with SLTT input) for when the federal government opens an investigation based on a referral from SLTT law enforcement and set policies for how to better support cases emanating from SLTT investigations.[91] The review process should consider whether regional thresholds need to be established to account for various demographics that exist across regions (e.g., rural vs. urban) and Recommendation 11.1's assessment.
- Create a uniform definition for cybercrime that the federal government can use for creating policies and informing data collection efforts and incentivize SLTT criminal justice partners to adopt a similar definition.[92] This definition could then be enumerated in a National Security Presidential Directive (NSPD), similar to NSPD 54, which defined "cyberspace."[93] With a definition, the federal government can better create specific policies, implement strategies, and design metrics around cybercrime.[94]
- Create a framework within which government agencies can assess (with input from private sector partners) ethical, economical, and global equities and determine whether a cybercrime incident is best mitigated through a traditional law enforcement approach, through a disruption operation with private partners, or a combination of the two. This framework should take into account the policies developed in Recommendation 1.5.

Objective 7: Increase prioritization of cybercrime among federal, SLTT, and private sector stakeholders and direct federal resources to federal and SLTT agencies that are commensurate with its prevalence and impact.

7.1 OMB and the ONCA should review all federal departments and agencies with cyber enforcement missions to create a comprehensive cyber enforcement budget proposal for the President's Budget Request for FY 2023 and/or FY 2024 (101–180 Days).

Federal departments and agencies responsible for cyber enforcement have seen flat or declining cyber enforcement budgets. Relevant entities within DHS, the FBI, and DOS have faced proposed or implemented budget cuts over the past few years, diminishing their capacity to train and engage domestic and foreign partners.[95] For example, the USSS National Computer Forensics Institute (NCFI), which offers training courses to SLTT personnel, requires $35 million to operate at full capacity, but was proposed to receive $4 million for FY 2021.[96]

Budget shortfalls at the federal level impact SLTT agencies as well, leading to fewer opportunities to train cybercrime investigators and prosecutors through programs operated by the FBI and USSS.[97] As a consequence of this lower spending, DOJ and DHS' grants awarded to nonprofits bear a heavier responsibility to fill the training gap, such as those provided to the National White Collar Crime Center (NW3C).[98]

With the President's FY 2022 budget proposal well underway, OMB should consult with the ONCA to create a comprehensive cyber enforcement crosscut for the President's Budget Request

for FY 2023 and/or FY 2024. For federal departments and agencies with cyber enforcement missions, the crosscut should, at the minimum:

- Detail the current resources allocated to the department/agency used for cyber enforcement purposes.
- Identify nonprofits whose work supports federal and SLTT criminal justice agencies and receive federal funding or grants, list the amount and source of federal funding, and identify how much funding is needed to operate at full capacity.[99]
- Identify existing grants that SLTT criminal justice agencies use for cyber enforcement missions, how much each SLTT entity receives, and how they use those funds for cyber enforcement initiatives (see also Recommendation 11.2).
- Request additional funding to reimburse federal entities for their detailees on interagency task forces. Specifically, DOJ should require the FBI to request additional funding in its proposed budget for FY 2023 to reimburse participating agencies for the detailees they send to the NCIJTF to support their interagency cyber enforcement efforts.

7.2 The ONCA should develop a plan to attend and hold a series of forums and workshops with SLTT and private sector participants to discuss the challenges to cyber enforcement and areas to improve partnerships (0–100 Days).

Since 2015, DOJ has held an annual "Cybercrime Symposium" to discuss cybercrime trends, challenges, and lessons learned with academic, private sector, and government practitioners.[100] The FBI, DHS's Homeland Security Investigations, and USSS have also held events with stakeholders to develop partnerships and reinforce the importance of cyber enforcement.[101] Additionally, the government convenes forums with nonprofit organizations like NW3C, which has brought together senior cybercrime investigators from each state every year since 2003 to discuss cyber enforcement challenges and solutions. Private sector companies, too, host numerous events throughout the year that federal government officials speak at to highlight their respective agencies' priorities and challenges.

The ONCA should coordinate with relevant federal departments and agencies to organize or participate in events to discuss the administration's cybercrime priorities and overcome challenges to strengthening partnerships. Departments and agencies that have hosted relevant events in the past should include in their FY 2023 and/or FY 2024 budget requests the costs to operate those events and potential new events.[102] The federal government should also host specific conversations on how to establish mechanisms to coordinate cyber enforcement actions with the private sector. Agencies should also identify annual association conferences[103] and private sector cybersecurity events[104] where senior government leaders can speak to further highlight the administration's efforts and promote partnerships.

Objective 8: Develop uniform metrics to inform and improve data reporting, victim response, and national data collection for federal and SLTT law enforcement.

8.1 The ONCA should consult with relevant federal departments and agencies to develop uniform metrics to evaluate the federal government's efforts to reduce cybercrime and to inform data collection efforts (101-180 Days).

The 2018 National Cyber Strategy listed objectives to reduce cybercrime, but no metrics to assess the federal government's efforts.[105] A 2020 GAO report found that due to the lack of metrics within the 2018 National Cyber Strategy, "[federal] entities may not understand what they should try to achieve or the steps required to produce the desired results."[106] Some departments and agencies—like DOJ and USSS—have created metrics related to prosecutions and the prevention of financial losses, but they may not provide a full picture of how effective the US government is at preventing and mitigating the consequences of cybercrime.[107] For instance, DOJ assesses its ability to recover private sector financial losses based on the FBI's Internet Crime Complaint Center (IC3) data, but given that IC3 accounts for only 10-12% of all reported cybercrime, achieving that metric may be inadequate.[108] Further, where these metrics do exist, they are spread out across various agency reports and do not reference each other, further impeding policymakers' ability to make informed conclusions on the US government's ability to reduce cybercrime.

The ONCA should consult with relevant departments and agencies to develop uniform metrics across the federal government. Specifically, the ONCA should:

- Consult with OMB to include in the cybersecurity crosscut (Recommendation 7.1) the metrics that departments and agencies with cyber enforcement missions will use to evaluate the impact of their efforts in reducing cybercrime and imposing consequences on perpetrators.[109]
- Include in the FY 2023 and/or FY 2024 Budget Request funds for the National Institute of Standards and Technology (NIST), or a grant for the National Science Foundation (NSF) or a federally funded research and development center (FFRDC), to conduct a study on the current mechanisms that the US government uses to measure and evaluate its effectiveness in combating other types of crime and determine whether they would be applicable to cybercrime.[110]
- Examine the benefits of moving to a harm-based approach to cybercrime and determine what other impacts, other than financial loss, should be considered when assessing the effect of cybercrime on specific victims (e.g., vulnerable populations).[111]
- Supplement traditional law enforcement metrics (indictments, arrests, convictions) with disruption-focused metrics (number of victim individuals/companies for whom risk is mitigated, number of networks defended, etc.) to assess if the expansion of disruption actions are warranted in defined cases, where more focused and unified disruption efforts could result in significant cost savings and protection of victims (see Recommendation 6.1).

8.2 The DOJ and FBI should develop policies and legislative proposals to expand cybercrime categories in the National Incident-Based Reporting System (NIBRS), further spur the uptake of NIBRS, and explore other initiatives to improve data reporting (1 Year+).

Traditionally, SLTT law enforcement agencies report crimes to the federal government through the Uniform Crime Reporting (UCR) Program, which collects data through the Summary Reporting System. The UCR is in the process of transitioning into a broader data collection system called NIBRS by January 2021.[112] Two prominent challenges, however, exist with NIBRS. First, of the 50+ offenses listed in NIBRS, only one—"hacking/computer invasion"—is designated for cybercrime, potentially leading to a vast undercount of its occurrence.[113] Second, only half of SLTT law enforcement agencies submitted data to NIBRS in 2019.[114] As a result, federal and SLTT leaders lack data to make informed policymaking decisions.

The DOJ and FBI should develop policies and recommend legislative proposals to overcome challenges associated with NIBRS by:

- Consulting with the Criminal Justice Information Services Advisory Policy Board (CJIS APB)[115] to review the National Academy of Science's 2016 and 2018 Modernizing Crime Statistics Reports' proposals on including cybercrime categories in NIBRS.[116] The FBI and CJIS APB should consider whether the proposal to use a yes/no flag to indicate if a crime was cyber-related and whether "the use of computer data or computer systems was an integral part of the modus operandi of the offense"[117] would sufficiently cover the most common cybercrimes identified by DOJ's 2018 Cyber Digital Task Force Report.[118] CJIS APB should also consider whether additional categories need to be included based on Recommendation 8.1.
- Clarifying and emphasizing that federal grants—like DOJ's Byrne Memorial Justice Assistance Grant (JAG) program and the State Justice Statistics Program for Statistical Analysis Centers[119]—can be used for cybercrime reporting efforts. Contingent upon assessments recommended in Objective 11, DOJ should also request more funding for those grant programs in their FY 2023 and/or FY 2024 and subsequent budget requests and, if granted, earmark a percentage of each grant to cybercrime data collection efforts.[120]
- Working with Congress to pass legislation, similar to the Hate Crime Statistics Act[121] and the William Wilberforce Trafficking Victims Protection Reauthorization Act,[122] to mandate the collection of cybercrime data through NIBRS. Any legislation should also ensure that federal agencies are required to report relevant data as well.[123]
- Requiring all federal law enforcement agencies and programs with cyber enforcement missions—including programs like IC3 and iGuardian—to report arrest, incident data, and clearance rates for cybercrime through NIBRS.[124]
- Returning the IC3 to the more detailed reporting it provided up through 2009, including details on perpetrators of cybercrime in cases where federal law enforcement has been able to investigate and identify them. This should also include requiring IC3 to report on the number of incidents that were investigated and those that led to an arrest or some form of enforcement action. This data should align with the NIBRS reporting framework.[125]

- Releasing the annual NIBRS report in conjunction with the FBI's annual IC3 report to provide a comprehensive overview of cybercrime until the IC3 data is accurately represented within NIBRS.[126]

8.3 To improve law enforcement's response to victims, the Cybercrime Working Group should develop proposals that improve cybercrime reporting among public and private victims and the assistance awarded to them. (1 Year+).

When asked what crimes Americans worry about, 72% of respondents reported concerns that hackers would steal their personal, credit card, or financial information, ranking it highest among a list of thirteen crimes.[127] They have reason; public polling reveals that roughly one in four Americans report that they or someone in their household has been a victim of cybercrime. Yet just 1 in 10 reports the crime to law enforcement,[128] and when they do, the laws and policies on victim restitution for cybercrime victims are unclear and limited.[129] Private companies, too, report infrequently due to concerns regarding bad publicity and the perception of working closely with law enforcement, which could lead to a loss in profits.[130] Still, federal and SLTT law enforcement efforts to report statistics and assess their efforts against cybercrime are only as good as the information they receive from victims.

When asked what crimes Americans worry about, 72% of respondents reported concerns that hackers would steal their personal, credit card, or financial information, ranking it highest among a list of thirteen crimes.

To improve data reporting of cybercrime incidents and bolster victim assistance, the Cybercrime Working Group should create policies and legislative proposals to:

- Update the 2012 Attorney General's Guidelines for Victim and Witness Assistance to explicitly account for victims of cybercrime outside of stolen personally identifiable information.[131]
- If needed, work with Congress to amend the Victims' Rights and Restitution Act and the Crime Victims' Rights Act —which accord certain rights to individuals who meet the statutory definition of "victim" and "harm"—to account for cybercrime.[132]
- Collaborate with DOJ's Office for Victims of Crime (OVC) to publish an updated rule that expands the eligibility of the Victim Assistance Program to include victims of cybercrime. The new rule should also detail allowable costs that include legal support services, mental health counseling, and other services as determined by OVC.[133]
- Assess ongoing efforts to establish a national call center, operated by the Cybercrime Support Network, for members of the public and small and medium-size businesses to report cybercrime and determine how a center would interact with other federal reporting mechanisms.[134]
- Review the FBI's implementation of the DOJ Inspector General's recommendations for improving the FBI's cybercrime victim notification process.[135]

- Identify potential victim-reporting challenges with the IC3 and the Federal Trade Commission's (FTC) Consumer Sentinel Network, including how the agencies interact with those who report a crime and how to deconflict their missions.
- Task DOJ's Bureau of Justice Statistics (BJS) to conduct a new National Computer Security Survey, which BJS last conducted in 2005, to identify the prevalence of cybercrime among individuals and the private sector.[136] DOJ should include funds in its FY 2023 and/or FY 2024 budget proposal to conduct this survey, which should be conducted every two years and allow for the anonymization of responses.[137]
- Provide revisions to DOJ's "Best Practices for Victim Response and Reporting of Cyber Incidents," which was last updated in 2015, to provide further information on how the federal government can assist victims of cybercrime.[138]
- Identify states that limit victim compensation only to victims of violent crime and encourage them to expand it to victims of cybercrime.[139]
- Create a public messaging campaign for victims on how to report cybercrime, where to report, and describe what happens once law enforcement receives the complaint to illustrate that law enforcement is taking action.

Objective 9: Strengthen federal and SLTT law enforcement's ability to share investigative information related to cybercrime.

9.1 The Cybercrime Working Group should develop policies and propose additional funding to strengthen existing information sharing mechanisms to enable investigations by criminal justice agencies (1 Year+).

Criminal justice agencies already share investigative information on traditional crime and cybercrime across federal and SLTT jurisdictional lines. The FBI houses the National Data Exchange System, eGuardian, the Malware Investigator, the National Crime Information Center, and a number of nonprofits, such as the National Cyber-Forensics and Training Alliance (NCFTA), also work to facilitate criminal justice agencies' ability to share, search, link, and analyze information in both unclassified and classified settings.[140] The FTC also hosts the Consumer Sentinel Network, which allows criminal justice agencies to search a database of scams and identify thefts.[141] SLTT law enforcement share information through local fusion centers and, in some cases, state-operated cybersecurity and communications integration centers.[142] States also maintain statistical analysis centers that collect, analyze, and share justice and crime statistics, which could be used to identify national and state-by-state cybercrime trends.[143]

The Cybercrime Working Group should take the following actions to strengthen existing information sharing mechanisms:

- Collaborate with states that have cybersecurity and communications integration centers[144] to identify best practices for how states can create or use existing institutions, like the Criminal Intelligence Coordinating Council and state fusion centers, to foster information sharing environments for cybersecurity and cybercrime.[145]

- Examine how existing investigative information sharing programs can become interoperable to foster users' ability to search and share information across various platforms.
- Identify and expand additional training on how to use these programs.
- Determine if stronger privacy requirements are needed for current and proposed investigative information sharing programs.

To encourage states to analyze and share cybercrime information, DOJ should also direct BJS to include cybercrime as a "topical area" in its annual State Justice Statistics Program for Statistical Analysis Centers grant program, where it has not been a topical area since at least 2009.[146]

Objective 10: Improve the digital evidence forensic capacity and capability of federal and SLTT criminal justice agencies by reforming recruitment, training, and retention practices.

10.1 The Office of Personnel Management (OPM) and OMB should issue a memorandum that outlines policy proposals and propose funds for FY 2023 and/or FY 2024 to improve recruitment practices for federal law enforcement agencies regarding cyber enforcement personnel (101–180 Days).

Roughly 32,000 cybersecurity jobs are open in the public sector, with nearly 3,000 of them related to analyst and investigative positions, according to Cyberseek, a grantee of the National Institute for Cybersecurity Education (NICE).[147] This is likely a vast undercount as "reliable, quantitative information about the cybersecurity workforce is lacking," according to DHS and the Commerce Department.[148] This undercount presumably pervades federal law enforcement agencies given that they must compete with the private sector, which can often offer better salaries. Further, women, minorities, and other underrepresented groups have not been adequately recruited from, as highlighted in Part 1 of this report, despite a body of research indicating that diversity leads to better outcomes. Previous administrations took steps to close the cyber-federal workforce gap, but those measures looked at cybersecurity more broadly and did not detail measures for cyber enforcement.[149]

OPM and OMB should issue a memorandum (similar to their 2016 memorandum)[150] for executive departments and agencies with law enforcement missions to improve recruitment for cyber enforcement personnel to:

- Include in the President's Budget Request for FY 2023 and/or FY 2024 additional funding to expand the CyberCorps: Scholarship for Service Program and work with NSF, OPM, and DHS—which operates the program—to prioritize schools that teach competencies relevant to cyber enforcement.[151]
- Work with DOJ to include in the President's Budget Request for FY 2023 and/or FY 2024 additional funding to expand the Student Computer and Digital Forensics Educational Opportunities Program, managed by DOJ's Bureau of Justice Assistance (BJA), to increase the number of students enrolled in digital forensic curricula at higher-education institutions.[152]

- Establish and/or expand rotational assignments for private sector, SLTT, and federal employees to rotate within federal and SLTT law enforcement agencies to fill short-term positions that may otherwise go unfilled.[153]
- Mandate that federal law enforcement agencies prioritize implementing the Federal Cybersecurity Workforce Assessment Act of 2015 (FCWAA) so that cyber enforcement positions within the federal government are aligned with the NICE Framework categories.[154] Fully implementing the FCWAA will help human resource managers identify talent gaps within agencies. Indeed, DOJ found that implementing the FCWAA for the FBI would help "support possible recommendations for introducing new job roles that will improve the FBI's ability to respond to Internet-enabled crimes and technologically advanced threat actors."[155]
- Expand the Pathways Programs—programs that include internships and opportunities for recent graduates—and apprenticeships for federal law enforcement agencies with cyber enforcement mission areas.[156]
- Improve diversity, equity, and inclusion recruitment methods to reach diverse pools of candidates who are underrepresented in the federal workforce by, for example, recruiting from historically black colleges and universities and engaging in K-12 outreach. The federal government should also continue its efforts to recruit veterans.[157]

10.2 In their updated memorandum, OPM and OMB should include policy proposals and propose funds to expand training opportunities for federal and SLTT law enforcement and other criminal justice agencies and retain those employees once trained (101-180 Days).

According to CyberSeek, 83% of online job listings for "cybercrime analyst/investigator" require a bachelor's degree.[158] Yet at the SLTT level, only 30% of officers have a four-year college degree and only half have a two-year degree.[159] As a result, a delta exists in the current education levels (at least at the SLTT level) and the competencies needed to perform duties related to cybercrime investigations. However, like other cybersecurity professions, not all law enforcement personnel need a four-year degree to perform cybercrime investigations; some may just need a series of trainings and certifications. Federally funded organizations—such as the NDCAC, NCFI, NW3C, the NCFTA, and others—are therefore paramount to filling this skills gap. Yet, as described in Part 1, some of these organizations, like the NDCAC and NCFI, have been defunded in recent years, limiting how many personnel they can train.[160] Even with trained personnel, however, public agencies struggle to retain trained employees, who are lured by higher salaries to the private sector.[161]

OPM and OMB should include in their updated memorandum (see Recommendation 10.1) a requirement that federal departments and agencies with cyber enforcement missions expand training opportunities for personnel and methods to retain them. Specifically, OPM and OMB should:

- Direct DOJ to include funding in BJS's budget request for FY 2023 to conduct a survey that assesses the competency level of SLTT criminal justice personnel to handle cybercrime cases.[162] Existing BJS surveys that include cybercrime questions, such as the 2019 National Survey of Prosecutors, could be used as

a model.[163] This assessment could help determine how much federal funding, including grants, should be requested for FY 2024 to sufficiently train personnel. In the meantime, DOJ and DHS should request funding in FY 2023 to replenish the funding that the NDCAC and NCFI have lost in recent years.

- Determine the best agency to create a federal clearinghouse on cybersecurity education, training, and workforce development programs that federal and SLTT agencies can use, with input from SLTT criminal justice agencies.[164]
- Review how to expand or create a program, in accordance with the NICE Cybersecurity Workforce Framework, within the National Centers of Academic Excellence—a program that provides accreditations to higher education institutions for incorporating cybersecurity curriculums—that is tailored specifically to cyber enforcement needs.[165]
- Expand the FBI's cyber certified training and certification program, Forensic Examiner Certification Program, Cyber Executive Certification Program, and USSS Basic Investigation of Computer and Electronic Crimes Program for federal and SLTT criminal justice personnel.[166]
- Identify federal and SLTT cyber ranges—virtual environments that provide individuals hands-on cyber experience—that could be used to train and certify law enforcement personnel.[167] OPM and OMB should also determine if programs like the FBI's Basic School Program, a two-week curriculum designed to instill cybersecurity fundamentals in all employees, can be a model for those ranges.[168]
- Introduce and/or expand programs to train existing federal law enforcement personnel with limited to no experience working on cybercrime cases, similar to the FBI's Workforce Training Initiative and On the Job Training Initiative.[169]
- Work with DOJ so that each US Attorney receives basic cybersecurity and cybercrime training.
- Include digital evidence forensics curricula and other relevant cyber enforcement courses in the Federal Cyber Reskilling Academy, a program dedicated to train current federal employees in non-IT fields to gain cybersecurity skills, to expand training opportunities for non-IT professionals.[170]

Lastly, once the FCWAA is implemented across federal departments and agencies, agencies should use existing hiring and pay flexibilities for cybersecurity positions by determining if there is "an urgent need" to fill cyber enforcement roles as identified by the NICE Framework.[171] If retention issues persist after existing authorities are used, federal agencies with these positions should seek legal authority from Congress to create incentive pay for cyber enforcement personnel in exchange for additional service, similar to the incentives pay enumerated under the Uniformed Services Code.[172]

10.3 The ONCA should work with Congress to develop legislation to ensure that federal and SLTT criminal justice agencies have access to technical assistance to examine digital evidence (0-100 Days).

According to a 2018 Center for Strategic and International Studies survey, only 45% of local law enforcement has access to adequate digital evidence resources.[173] A 2014 DOJ survey also found

that despite 79 publicly-funded crime labs offering dedicated digital evidence support services, large geographical areas exist that require personnel to travel "far distances if they seek the kind of assistance that cannot generally be provided remotely."[174] For nearly every crime involving digital evidence, this lack of forensic capabilities creates bottlenecks that can delay investigations.[175]

To address these challenges, the ONCA should work with Congress to draft legislation with provisions similar to those in the Technology in Criminal Justice Act of 2019.[176] These provisions should include promoting public-private partnerships to improve law enforcement's access to digital forensics technology, reviewing federal assistance to SLTT partners, and creating and leveraging grant programs to support training, education, and technical assistance for criminal justice personnel to improve their capacity to analyze digital evidence. Grant programs that enhance SLTT digital forensic capabilities should also require grantees to create policies that retain digital evidence for an appropriate period and preserve suspect, victim, and third party privacy.

Additionally, the ONCA should work with Members of Congress to re-authorize the NCFI, which is set to expire in 2022, and ensure it has the required resources to fulfill its mandate.[177]

10.4 DOJ should develop policies and request sufficient funding so federal and SLTT criminal justice agencies have access to technical assistance to examine digital evidence (0-100 Days).

While the above legislation is pending, DOJ should also develop similar policies and request funding to advance these goals.

Specifically, DOJ should:

- Recommend, either by developing and/or identifying existing certification programs, voluntary guidelines for personnel who handle digital evidence and for prosecutors, defense attorneys, and judges who use it during court proceedings. These guidelines should also include an overview of cases relevant to digital evidence extraction and handling.[178] Contingent upon the assessments recommended in this roadmap, DOJ should also request additional funding for relevant grants to train SLTT criminal justice personnel towards the certification.[179]
- Request funding in the FBI's budget request for FY 2023 or FY2024 to create and/or expand Regional Computer Forensic Labs—17 federal labs that the FBI manages that convenes federal and SLTT law enforcement agencies to conduct digital forensics activities and assist in investigations—to ensure SLTT law enforcement officials have timely access to their services.[180]
- Direct the BJA to encourage grantees to the Paul Coverdell Forensic Science Improvement Grants Program to use their funds to support and/or create digital forensics labs. Contingent upon the assessments recommended in this Roadmap, DOJ should also request additional funding for this grant program in FY 2023 and/or FY 2024 to support additional funds for these purposes.[181]

Objective 11: Assess the needs, resources, and capacity of SLTT criminal justice agencies and federal-state collaborative organizations to address cybercrime.

11.1 DOJ should coordinate with DHS to assess the gap between the needs of SLTT criminal justice agencies and their capabilities and capacities. (0–100 Days).

In 2013, the Police Executive Research Forum conducted a survey of SLTT law enforcement on their cybercrime capabilities[182] and found significant challenges, including a lack of staffing, funding, and in-house experience. Alarmingly, one county stated that their clearance rate for cyber-related cases was only 10%. These agencies also heavily relied on federal agencies; 66% of SLTT respondents referred cases to the FBI, 51% referred them to the USSS, and 30% to federal task forces.[183] Yet, these agencies are not at fault due to the challenges and environments that have been previously discussed: a federal reporting system that does not prioritize or calculate the occurrence of cybercrime, a lack of metrics to assess their efforts, victims not reporting crimes, and prioritization of other issues at the SLTT level.

Due to limited survey data, the federal government lacks insight into their SLTT partners' ability to receive, investigate, and prosecute cybercrime at a macro level. As a result, the federal government and Congress does not have the data it needs to inform good policies, laws, and funding decisions.

DOJ and DHS should perform a needs assessment to examine SLTT criminal justice agencies' ability to:

- Access and analyze digital evidence.
- Provide the required data to NIBRS per Recommendation 8.2.
- Train law enforcement personnel on "basic" cyber enforcement operating procedures, such as how to handle digital evidence and submit digital evidence requests to providers.
- Train attorneys (including public defenders), prosecutors, clerks, and judges on how to use and interpret digital evidence during judicial proceedings.
- Engage with federal agencies on cybercrime cases (see Recommendation 11.3).

To conduct this assessment, Congress could consider providing a grant to a nonprofit organization or require the assessment as a condition of grant funding.[184] This assessment should also take into account any proposals developed under Recommendations 6.1 and 11.3 that focus on federal and SLTT coordination.

11.2 DOJ should determine how many localities are using the JAG program for cybercrime initiatives, how much these localities have received for these initiatives, how the program could be used to promote SLTT cyber enforcement, and whether other grant programs should be expanded (0–100 Days).

While several federal grant programs exist that SLTTs rely upon for a variety of needs,[185] DOJ's BJA primarily provides federal criminal justice funding to SLTT entities through the JAG program. These funds are used to provide additional personnel, equipment, supplies, contractual support, training, technical assistance, and information systems.[186] BJA also lists

"JAG Areas of Emphasis" to "encourage state and local jurisdictions to support projects" based on BJA's priorities. None of these cover cybercrime.[187] The amount that states are allotted is based on the state's population and the number of reported violent crimes in the state (Part 1 Crimes as collected by UCR/NIBRS).[188] JAG does not preclude SLTT agencies from using funds for cybercrime needs, but notwithstanding Americans' heightened concern about falling victim to cybercrime, combating cybercrime is deprioritized compared to violent crimes.[189]

To ensure that JAG emphasizes cyber enforcement, DOJ should direct BJA to:

- Review previous grant awards to determine how many applicants have used JAG grants to improve their cyber enforcement capacities and the total amount of JAG funds used for those purposes.
- Include cyber enforcement initiatives as an "Area of Emphasis" for FY 2021 JAG grants and future JAG grants.
- Encourage grant applicants to add an addendum to their JAG strategic plan to describe how this funding could be used to bolster their cyber enforcement capabilities through FY 2024.[190]
- Explicitly detail in the Notice of Funding Opportunity that cyber enforcement tools, programs, initiatives, and personnel can be funded by JAG, provided that applicants can show how they would sustain such programs and personnel, either through future JAG funding or SLTT expenditures.[191]
- Collaborate with the FBI and the CJIS APB to consider including categories of cybercrime as Part 1 crimes to encourage SLTT agencies to report cybercrime through NIBRS and to ensure that funds are allocated to those areas with high rates of cybercrime. Alternatively, BJA, FBI, and the CJIS APB could work with Congress to amend the JAG statute to include rates of cybercrime as part of the formula for allocating JAG funds to states.[192]

DOJ should also examine other grants, like the Community Oriented Policing Services program, to determine if they can emphasize and/or include cyber enforcement funding opportunities.[193] And as mentioned previously, DOJ should look at other BJA and National Institute of Justice grants, like the Student Computer and Digital Forensics Educational Opportunities Program, State Justice Statistics Program for Statistical Analysis Centers, and the Paul Coverdell Forensic Science Improvement Grants Program, to develop SLTT capabilities and capacity.

11.3 DOJ and DHS should identify and recommend proposals on how to improve federal and SLTT investigative and prosecutorial coordination (0-100 Days).

Because cybercrime crosses various geographical and legal jurisdictions, the federal government has created and expanded several cybercrime task forces throughout the states to foster collaboration. However, monetary thresholds prescribe when federal agencies get involved, and as a result cases that don't meet that threshold are often left unresolved due to limited capacity at the local level.[194] Further, the DOJ Inspector General found that attracting participants to engage in task forces, like the FBI's Cyber Task Force, is difficult because SLTT law enforcement agencies "believe that cyber intrusion investigations are inherently a federal matter, or [lack] the resources or personnel to detail an officer to the local Cyber Task Force."[195]

To foster federal and SLTT law enforcement coordination and partnership, DOJ and DHS should examine the FBI's Cyber Task Forces,[196] the Internet Crimes Against Children Task Force Program,[197] the FBI's Violent Criminal Apprehension Program,[198] Joint Terrorism Task Forces,[199] the USSS Cyber Fraud Task Force,[200] and other task force models to assess what current collaboration vehicles can be enhanced to strengthen federal and SLTT coordination. This examination should also include incentives for SLTT law enforcement agencies to participate in task forces, as lack of resource incentives has been a repeated obstacle for participation.[201]

Global Cybercrime Cooperation

Objective 12: Establish a new DOS structure to ensure a well-resourced single point of high-level leadership for all cyber diplomacy matters, backed by an architecture that allows for other bureaus advancing policy and programming on cybercrime to effectively coordinate.

12.1 The Secretary of State should establish an Office of International Cyberspace Policy at DOS with the head of Office having the rank and status of Ambassador and ensure this Office is supported with the adequate funding and personnel to fulfill its mandate (0–100 Days).

The Office of the Coordinator for Cyber Issues was established in February 2011 to spearhead DOS's global diplomatic engagement on cyber issues and coordinate the work of DOS's many regional and functional bureaus that are engaged in these areas.[202] The United States was the first country to establish such a senior-level official, who was given the title of coordinator. The Office has since been downgraded and placed within the Bureau of Economic and Business Affairs, eliminating its direct connection to the Secretary and sending a signal to America's allies, partners, and adversaries alike that cyber diplomacy is not a top priority for the US government.

Given the proliferation of cyber threats facing the United States and the lack of top-level US diplomatic leadership on these issues, the Secretary of State should establish an Office of International Cyberspace Policy at DOS led by an experienced official appointed by the President with the rank and status of Ambassador to restore America's leadership globally on cyber diplomacy. The Office should be established in such a way to ensure it:

- **Has direct access to the Secretary.** The Secretary should consider whether the Office for International Cyberspace Policy should be made a full DOS bureau and whether the head of such an Office should be appointed at the rank of Assistant Secretary or higher.[203] While this position may report to an Under Secretary, it could also be given the authority to report directly to the Secretary without the approval or concurrence of any other official at DOS, as threats and circumstances require.[204] Should the position report to an Under Secretary, consideration should be given to the chain of command that best ensures it has cross-cutting authority as referenced below.
- **Has cross-cutting authority to coordinate DOS's efforts on the full spectrum of international cyberspace policy issues, including cybercrime.** The Office should have duties such as those outlined in the bipartisan Cyber Diplomacy Act of 2019 to oversee all aspects of international diplomacy related to cybercrime,

cybersecurity, deterrence, Internet access, Internet freedom, the digital economy, the development of international norms of responsible state behavior in cyberspace, and other emerging challenges facing the United States in cyberspace.[205] This should also include ensuring the head of Office is able to:

1. Serve as the principal cyberspace policy official, including on cybercrime, within the senior management of DOS and as the advisor to the Secretary of State for cyberspace issues;
2. Serve as the principal advisor on cyber threat prioritization within DOS and ensure that the various bureaus and offices adopt plans in line with this prioritization and dedicate the needed attention and resources they deserve;
3. Lead DOS's diplomatic cyberspace efforts, including on cybercrime, in coordination with other DOS bureaus and offices, as well as other executive departments and agencies of the US government, or support other federal entities when more appropriate for them to lead such diplomatic engagement;
4. Advocate for the inclusion of cyber priorities in rule of law programming administered or supported by all DOS regional and functional bureaus and promote this in engagement with corresponding assistant secretaries;
5. Promote the building of foreign capacity on cyber, in coordination with other DOS bureaus and executive entities, and support the establishment of clear metrics to monitor and evaluate the effectiveness of such capacity building;
6. Promote and protect the exercise of all human rights and respect for the rule of law and civil liberties, including by supporting and consulting civil society groups working to advance such efforts, and considering strategies for mitigation on the misuse of capacity building, technical assistance, technology, and other areas of support provided by DOS to foreign governments; and
7. Promote diversity, equity, and inclusion within the Office of International Cyberspace Policy staff—including through increasing the participation of more women, minorities, and other underrepresented groups—and encourage such representation in international cyber forums and programs, policies, and initiatives administered by DOS to build foreign cyber capacity.[206]

- **Has sufficient personnel to fulfill its mandate.** The Secretary should ensure the Office is headed by an individual with experience on cyber issues and diplomacy and is sufficiently staffed to fulfill its mandate and the objectives of an updated International Cyber Engagement Strategy (see Recommendation 13.1 below). The Secretary should task all heads of Department bureaus and offices with appointing a senior-level person to serve as their representative to the Office of International Cyberspace Policy and attend meetings as requested.[207]

- **Has the authority to offer input into how cyber funding is spent by the Department.** The Office, in coordination with the Office of Foreign Assistance and Office of Budget and Planning, should task all bureaus and offices along with all entities at the US Agency for International Development (USAID) with assessing how much of their previous fiscal year budget was spent on any cyber-related programming, personnel, or policy efforts.[208] With this baseline, budgetary tracking systems should be updated so the Office of International Cyberspace Policy can receive annual updates and establish a process to provide input into how general funds, such as Economic Support Funds, are disbursed to functional and regional bureaus to ensure cyber issues are prioritized. The Office should also work with relevant department stakeholders to develop a universally accepted definition of "cyber," accounting for the federal government definition of cybercrime in recommendation 6.1, to assist and enable bureaus and offices to track cyber spending.
- **Has the authority to set overall key indicators and performance goals related to cyber and to coordinate with other functional and regional bureaus on their cyber-related indicators and performance goals.** DOS's annual performance report includes cyber-related performance goals and indicators.[209] Not only should the Office have the authority to set such indicators and performance goals, but functional and regional bureaus should be required to consult with the Office before setting any cyber-related indicators and performance goals.
- **Serves as the co-chair of all international cyber interagency policy committee (IPC) meetings, if appropriate in the broader IPC process.** IPC and sub-IPC meetings serve as an important forum for key officials and experts inside of the US government across departments and agencies to discuss cybercrime and other cyber-related threats that require international cooperation to address. To the extent it is appropriate in the broader IPC process, the Office should serve as the principal co-convener of such IPCs along with the proposed ONCA (see Objective 1) at the White House.

12.2 The White House should work with Congress to codify the Office of International Cyberspace Policy at DOS (0-100 Days).

Disagreements between DOS and Congress have prevented legislation from moving forward that would codify this Office. We believe the approach of the Cyber Diplomacy Act should be a baseline for future legislation. This legislation should ensure the Office is not placed in a chain of command at DOS that may inhibit work on the wide range of issues required to make progress on cyber enforcement while safeguarding human rights and promoting the rule of law.

Objective 13: Identify a set of diplomatic tools and policy options to boost international cooperation in cybercrime investigations and address governments that are systematically uncooperative.

13.1 DOS, in coordination with the White House and all relevant departments and agencies in the US government, including the IC, should draft a new US global cyber engagement

strategy through an interagency process. This strategy should be updated every four years and inform the development of a national cyber strategy by the White House (1 Year+).

DOS previously led an interagency process to draft an Engagement Strategy for International Cooperation in Cybersecurity, which was incorporated into the 2018 National Cyber Strategy.[210] DOS should lead an interagency process to draft a new global cyber engagement strategy that includes both public and classified portions and a corresponding implementation plan. This process should align with the ONCA's update of the National Cyber Strategy (see Recommendation 5.3). The NIE called for in Recommendation 4.5 should be conducted before the global cyber engagement strategy and transmitted to DOS to inform the development of this strategy.

This new global cyber engagement strategy should cover the full spectrum of cyber-related priorities for the United States, recognizing that cybercrime has not received the attention it deserves in previous DOS strategies and must be a central focus of this and any other cyber-related strategies moving forward. This strategy should include:

- An assessment of the goals, objectives, and indicators that will be used to guide the US government's efforts to promote a free, open, and secure Internet, expand the US government's allies and partners on cyber-related issues, and induce behavior change in states playing a role in cybercrime and/or other forms of malicious cyber activity.
- An evaluation of the effectiveness of current and previous US bilateral and multilateral diplomatic engagements in expanding US partners and allies on cyber-related issues, and a strategy for strengthening such efforts, including a determination of how the US government can be more active in pushing international organizations to expand their cybercrime engagement.[211]
- A strategy for DOS and DOJ to work together to increase the number of Member States that accede to the Convention on Cybercrime of the Council of Europe (Budapest Convention).[212] This should include an assessment of the effectiveness of US government messaging on the benefits and opportunities afforded to States that join the Budapest Convention and of US capacity building efforts and technical assistance to facilitate membership in this Convention.
- An evaluation of whether DOS's current level of resources, both in budget and personnel, is adequate to achieve the stated goals and objectives. DOS should also assess whether it currently has the level of expertise in key bureaus and missions, particularly missions to the UN and other international organizations, needed to advance US priorities on cybercrime, cybersecurity, and other cyber issues.
- A classified annex with an individualized plan for each country the IC determines is abetting, ordering, or conducting cybercrime and/or other forms of malicious cyber activity, including objectives for deterring and responding to such activity, tools to deploy to do so, and clear roles and responsibilities assigned to entities in US government departments and agencies.
- A classified list of principles, which could include general talking points, to guide heads of state or minister-level engagement by the President or Secretary of State, Attorney General, or other cabinet-level officials with foreign counterparts

to raise cybercrime and other cyber-related diplomatic priorities, including accession to the Budapest Convention.

- An implementation plan and timeline that includes an assigned lead implementing entity in the US government and budgetary estimates where applicable.
- A delineation of the roles and responsibilities on global cyber engagement, including cybercrime, throughout the US government as determined by the ONCA (see Recommendation 6.1). This should include a plan for strengthening cooperation, coordination, and transparency on these issues between DOS and USAID.
- A plan for formalizing the DOS's engagement with the private sector and civil society groups on global cyber issues. This may involve soliciting their views on bilateral and multilateral negotiations, when appropriate, and discussing partnerships to promote responsible state behavior in cyberspace and advocating for behavioral change in states that are systematically unwilling to cooperate in cybercrime investigations. This engagement should also explore how US-funded foreign cyber capacity building programming can better align with new technological developments and best practices in cybersecurity.[213] In establishing this plan, DOS must recognize that the "private sector" and "civil society" are not monoliths and ensure diversity in representation and perspectives.
- A plan to strengthen US leadership in forums aimed at establishing cyber norms, rules, and principles to guide state behavior in cyberspace. This should include the promotion and enforcement of norms previously agreed upon, consideration of US membership in the Paris Call for Trust and Security in Cyberspace,[214] and promotion of the norms established by the Global Commission on the Stability of Cyberspace.[215] The US government should continue to reaffirm international law is applicable to cyberspace and impose consequences on states that violate international norms, particularly those that disrupt or attack critical infrastructure. Norms on cybercrime cooperation have largely remained voluntary and non-binding for many reasons, including that cybercrime has historically been viewed as a tool of non-state actors. With the increasingly blurred line between state and non-state actors on cybercrime, such a plan should detail how the US government might work to strengthen such norms on cybercrime cooperation and explore links between norms of state behavior and cyber stability and those on cybercrime. It should also assess how partnerships with the private sector and civil society can be better leveraged to enforce these norms.[216]
- A recognition that the US government must engage with foreign governments on cyber-related issues in a reciprocal fashion. The United States has often made demands of foreign governments that it is not able or willing to uphold itself, such as in the timely response to cross-border data requests or the implementation of cyber norms, rules, and principles guiding state behavior in cyberspace. If the US government wants to advance cooperation with foreign governments on a wide range of cyber issues, then it must be willing to assess areas where its own actions might hinder progress.

13.2 Once a new global cyber engagement strategy is issued, all regional DOS bureaus and USAID should update or draft regional cyber strategies to align with the newly established goals and objectives (1 Year+).

DOS has previously created regional cyber strategies to implement its global cyber strategy.[217] These bureaus should be required to draft new or update previous regional cyber strategies to align with a new DOS-wide cyber engagement strategy, and do so following all subsequent strategy updates every four years.

13.3 DOS should include cybercrime and other cyber priorities in other key review and strategic planning documents for the Department and USAID. This should include any and all future Quadrennial Diplomacy and Development Reviews (QDDR) (1 Year+).

In addition to issuing a new global cyber engagement strategy and setting specific cyber performance goals and indicators, DOS should include a specific component on cybercrime and other cyber issues in all DOS strategic review and planning documents. If DOS conducts another QDDR,[218] it must ensure that cybercrime, cybersecurity, and other cyber issues be a key standalone priority. While the 2010 QDDR laid out the case for an Office of the Coordinator for Cyber Issues and highlighted the need to work through NATO and with NATO allies to boost cyber capabilities,[219] the 2015 QDDR only made passing reference to this priority. The world has changed dramatically since this last QDDR, with increasingly blurred lines between state and non-state malicious cyber activity, growing digital authoritarianism, and a fragmenting of cyber norms. Any future QDDR or other strategic planning and review processes must reflect these developments and describe how DOS will meet the objectives established in the global cyber enforcement strategy, including through bureaucratic and institutional reforms and dedicated resource streams.

13.4 DOS should enhance its training and awareness raising on cybercrime for policy officers at posts, encourage posts to add cybercrime as a standing item to Law Enforcement Working Groups, identify additional Department-wide training opportunities to enhance training and awareness on cybercrime, and dedicate time at annual Chiefs of Mission meetings for updates on cyber developments (101-180 Days).

DOS should improve its training on cybercrime-related issues for policy officers sent to posts and highlight the role of and support that can be provided by DOJ, FBI, and other US government personnel at posts in cybercrime cases. DOS should also encourage posts to add cybercrime as a standing item for their Law Enforcement Working Group. The Office of International Cyberspace Policy should also identify additional DOS-wide opportunities to train and raise awareness of cybercrime issues among personnel, including those in the Foreign Service. Further, the head of the Office of International Cyberspace Policy should be invited to present on global cyber developments, including trends in cybercrime, before the annual Chiefs of Mission meeting whenever possible and relevant.

13.5 The Department of Treasury, in coordination with all other relevant departments and agencies including the IC, should undertake an inter-agency assessment of the effectiveness of all existing cyber-related sanctions in halting or reducing malicious cyber activity (101-180 Days).[220]

It has been over five years since President Obama issued the first executive order to establish a dedicated cyber sanctions regime in the United States. Since then, the Treasury Department

has largely imposed sanctions under this regime on individuals and entities in four countries: Iran, Russia, North Korea, and China.[221] A review of these sanctions indicates an overwhelming majority are suspected of having links to nation-state entities.[222] With the European Union (EU) following suit last year, the United Kingdom moving forward with its own cyber sanctions regime, and the Treasury Department's June 2020 announcement that it has sanctioned six Nigerian nationals for a cybercrime scheme,[223] the time is ripe for an inter-agency, holistic assessment of the impact of US cyber-related sanctions. The Treasury Department should institutionalize this review every four years, in conjunction with the update of DOS's global cyber engagement strategy (see Recommendation 13.1) and the White House's National Cyber Strategy (see Recommendation 5.3).

Such an assessment should include:

- A determination of the effectiveness of sanctions in changing or deterring behavior of the intended target(s). And if such behavior has neither changed nor been deterred, an IC evaluation as to why not. This determination should take into account any relevant research from outside the US government.
- An evaluation as to whether the issuance of further cyber-related sanctions could weaken or strengthen existing sanctions, including consideration of IC assessments on the expected reciprocal actions from the targeted actors or governments.
- Based on the above evaluation, a determination as to whether the decision-making framework for the issuance of cyber-related sanctions should be updated.
- An analysis of the application of sanctions to target non-state cybercriminals and the expected outcome of such a tool on non-state actors.
- A strategy for US diplomatic efforts to advocate for additional cyber sanctions regimes in non-EU countries, including considering whether the US government should advocate for a multilateral cyber sanction regime.
- An assessment of the effectiveness of the US government's public or private messaging on individual(s) or organization(s) currently sanctioned for malicious cyber activity, including the specific behavior that such sanctions are targeting and how changes in their behavior will lead to a lifting of sanctions.

13.6 DOS, in cooperation with the Department of Treasury, should increase support to non-governmental research institutions to conduct regular, independent assessments of the effectiveness of cyber sanctions and propose recommendations to improve the US's cyber sanctions regime (1 Year+).

GAO found in 2019 that US government agencies have not determined whether sanctions actually "work" and are not required to do so.[224] As cyber sanctions have increasingly become a tool in America's cyber diplomacy toolbox, agencies should invest resources to study whether these sanctions are working. Fortunately, there are numerous FFRDCs, non-profit think tanks, and academic institutions with the necessary expertise on US sanctions policy. Instead of solely relying on the US government's own internal assessment of its cyber sanctions efforts, DOS, in partnership or cooperation with Treasury, should support institutions doing regular, independent expert evaluations on the effectiveness of US cyber sanctions.[225]

GAO found in 2019 that US government agencies have not determined whether sanctions actually "work" and are not required to do so.

13.7 Should the United States choose to participate in negotiations on a new global cybercrime convention, it should develop a strategy for engagement and ensure the process is transparent, inclusive, and safeguards human rights (1 Year+).

Negotiations on a new global cybercrime treaty, sponsored by Russia, may begin in earnest in 2021. The US government unsuccessfully opposed a UN General Assembly resolution in 2019, which was sponsored by Russia and had the support of China and a number of other Member States, to begin negotiations on a treaty.[226] Such a treaty threatens to undermine progress that has been made on the Budapest Convention. Human rights and other civil society organizations have expressed deep concerns about the framing of the Russian resolution and draft treaty provisions Russia previously circulated.[227]

A determination by DOS as to whether the United States will participate in substantive negotiations should be made after the process and procedures are established. If the US government chooses to participate, it should develop a strategy for achieving US objectives, including the following actions:

- DOS should be the lead US government agency in these negotiations, supported by DOJ and any other relevant US government entities as necessary. DOS should designate a senior-level official as the lead negotiator and ensure that the UN's secretariat and the chair of any negotiations have a direct line to this individual and/or their staff.
- The US government, led by DOS in partnership with DOJ, should work with allies and partners to push for a formal consultative mechanism to ensure private sector and civil society organizations can share their recommendations, perspectives, and concerns throughout the negotiation process and are well briefed on developments in the negotiations. Without input and partnership from the private sector and civil society, any binding mechanism for global cybercrime cooperation will be wholly ineffective.
- The US government should advocate for strong human rights and rule of law safeguards that, at a minimum, meet the safeguards required for membership in the Budapest Convention and look to go even further. The US government position should reflect its regular consultation with groups focused on digital and human rights (including those focused on gender, civil liberties, and digital and racial equality) and other particularly affected constituencies.
- The US government should be prepared to walk away from such negotiations if it becomes clear that strong safeguards to protect human rights, democracy, and the rule of law will not be considered.

Objective 14: Identify a group of countries where the US government is not receiving timely assistance in cybercrime investigations and develop programs to support their criminal justice capacity building needs—including operational support, policy development, and harmonization of laws—to boost cooperation.

14.1 As part of the development of a new global cyber engagement strategy, DOS should work in cooperation with USAID, DOJ, FBI, the IC, and all other relevant federal entities to develop an assessment, monitoring, and evaluation (AM&E) framework for all cyber foreign capacity building programs funded through annual foreign assistance resources. This AM&E framework should inform and ultimately be integrated into a broader DOS security-sector assistance AM&E framework (181 Days – 1 Year).[228]

Despite progress, DOS still lacks a comprehensive, holistic AM&E framework that is universally used across DOS for security assistance programming. This hinders DOS's ability to determine the efficacy and impact of all foreign assistance programming aimed at building partner governments' security capacity. Developing a universal framework will take time and resources, but DOS can immediately begin developing an AM&E framework specifically for cyber foreign capacity building programs that includes cybercrime as a critical area of focus and that aligns with any work underway to develop a universal framework.[229] A cyber AM&E framework would enable more informed decisions on the allocation of resources, inform the prioritization of certain countries and capacity building areas, and allow for a regular, systematic evaluation of cyber capacity building programming. Establishing a cyber AM&E framework will take a significant amount of time and resources, but without it DOS will be unable to assess the impact of its cyber capacity building even as cyber threats become a predominant national and economic security threat for many countries. As such, DOS must dedicate adequate personnel and funding to establish this framework and ensure such resources are reflected in the annual budget submitted to Congress if necessary.

DOS should ensure that an AM&E framework for cyber is aligned with what should be a Department-wide AM&E framework for all security assistance programs. Otherwise, DOS will be less able to measure progress and impact of cyber capacity building in relation to other security assistance programs, leading to a piecemeal approach to capacity building in recipient countries.

The US government has invested foreign assistance resources into programs aimed at enhancing the capacity and capability of foreign criminal justice entities—particularly investigators, computer forensic experts, and prosecutors—to investigate and prosecute cybercrime and develop regional and global networks to assist in these efforts. However, a more comprehensive framework than what currently exists is needed to determine the size, scope, and impact of such programming and all cyber capacity building programming resourced through foreign assistance accounts.

The establishment of a cyber capacity building AM&E framework should:

- Include a baseline assessment and allow for further regular assessment of all cyber capacity building programs and their corresponding budget levels (whether funded by State or Foreign Operations resources).[230]

- Establish a minimum monetary threshold for capacity building projects that will be required to be assessed and use the established AM&E framework for cyber capacity building programming. Such a minimum monetary threshold should ensure at least half of cyber capacity building programs and projects supported by foreign assistance funding would be required to use this framework.
- Document all federal bureaus and offices that support and/or implement significant cyber capacity building initiatives, including those focused on bolstering the capacity of global criminal justice actors to fight cybercrime and other malicious cyber threats.
- Set short, intermediate, and long-term objectives for each program or project and regularly assess whether objectives are being met. Such objectives could include building or strengthening support for the US government's broader goals to promote a free, open, and secure Internet.
- Evaluate, as informed by any relevant IC analysis, the likelihood that objectives will be met and the potential impact on security sector politics and human rights. This will ensure that cyber capacity building programs do not have unintended impacts on broader US government objectives and that an AM&E framework can be used to regularly monitor potential abuse or misuse of such programs (as has been observed in a number of countries).[231] Such an assessment should inform metrics that will allow program managers to monitor and evaluate whether unintended consequences are occurring and set guardrails to discontinue support if needed.
- Require all assessments, starting with the program design phase, to integrate a gender analysis to assess the potential impacts of security assistance programming on women and men, girls and boys, in line with the commitments in the Women, Peace, and Security Act of 2017[232] and analyze the differential impacts of such programming on other social identities.
- Align with all existing DOS monitoring and evaluation framework processes[233] and establish a baseline and indicators to track and measure progress and impact toward set targets while accounting for human rights safeguards and gender considerations. This should allow for a regular examination of the effectiveness and impact of such activities and programs based on these indicators in meeting the established short, intermediate, and long-term objectives. Monitoring and evaluation of programs and projects should consider whether any unintended consequences have resulted from capacity building and, if so, allow for funding to be halted or paused.
- Allow for annual evaluation of programs and for results to be transmitted to DOS's Office of International Cyberspace Policy, which should use this data, in coordination with other DOS offices, to inform decision-making on the distribution of cyber-related foreign assistance funds.

14.2 The Office of International Cyberspace Policy, in partnership with the International Narcotics and Law Enforcement Bureau (INL) and relevant federal entities, should lead a process that identifies a target number of countries where the US government is not

receiving timely assistance in cybercrime investigations and increased support to their cyber capacity building needs may have an impact (1 Year+).

DOS's INL Bureau receives funding for cybercrime and intellectual property rights (IPR) global capacity building programs through the annual state and foreign operations appropriations bill. However, DOS has attempted to cut the request for this line-item from $10 million to $5 million for the past three fiscal years.[234] Fortunately, Congress has not fulfilled this request; however, this existing funding pales in comparison to the capacity building support provided for other security threats, such as terrorism.[235] The continued global cyber enforcement gap makes clear that more capacity building is needed to strengthen the capabilities of governments to combat this threat.[236]

As part of the drafting of the global cyber engagement strategy (see Recommendation 13.1) and informed by the IC assessment on cybercrime (see Recommendation 4.5), DOS, DOJ, and other relevant federal entities should identify a group of countries where national laws criminalize cybercrime acts as defined by the Budapest Convention (or at least some initial steps have been taken in the direction of such criminalization), but the country's government has been unable to stop malicious cyber activity at least in part due to issues around inadequate capability and/or policy or legal constraints. This should include governments that are not members of the Budapest Convention, but that DOS determines may be willing and able to meet the qualifications for membership in the future if they have increased capacity to do so.

- Once this group of countries is identified, DOS and DOJ should determine a set of criteria—including the importance of each country to broader US government foreign policy objectives—to be used to select countries for a pilot program for cyber capacity building, with a substantial focus on strengthening cybercrime enforcement capacity. To ensure the effectiveness of such a pilot program, no more than 10 countries should be selected, with a focus on ensuring as much regional diversity as possible.
- DOS and DOJ should work through an interagency process to identify the top capacity building needs of these governments, including operational support, policy development, and harmonization of laws, and either plan to increase bilateral funding toward these efforts or, when appropriate, provide support through international organizations such as the UN.
- DOS should include in its annual congressional budget justification a funding request for this pilot program, plus the additional staffing necessary to support it, and an explanation for how the countries were selected, including how IC analysis informed the process. A classified annex with more specific analysis can be sent to Congress separately.
- The Office of International Cyberspace Policy; INL; the Bureau of Democracy, Human Rights, and Labor; and other key DOS entities should work in cooperation with Congress to identify any areas in existing law that may require changes to allow the US government to build the cyber capacity of security sectors, while still ensuring repressive governments or their institutions are not given support and tools to perpetrate abuses.
- The established AM&E framework should be used to conduct an assessment for each selected pilot program country and monitor and evaluate capacity building

efforts annually to assess the impact and effectiveness of such efforts in meeting the established objectives. Should a majority of the short, intermediate, and long-term objectives be met, DOS should look to institutionalize this pilot program as part of the Cyber and IPR global programming executed by State INL and increase its budget and personnel accordingly.

14.3 DOS should take steps to establish regional and/or in-country donor coordination mechanisms on cyber capacity building to overcome the duplication in funding that has been observed from donor governments (1 Year+).

Research has found that the sheer number of global organizations that are involved in cyber capacity building makes coordination among donors particularly difficult.[237] This can make it challenging to ensure the US government is funding capacity building programs that do not duplicate other donor-supported programs or, worse, work at cross-purposes to each other.

To help overcome these issues, the US government should establish regional donor coordination mechanisms to share more information about its priorities, programming it supports, and the key actors on the ground with which it liaises. DOS should assess whether existing mechanisms such as the US Transnational and High-Tech Crime Global Law Enforcement Network could work to coordinate donors across different regions.[238] Additionally, DOS should encourage its overseas missions to establish in-country donor coordination mechanisms for cyber capacity building and send guidance to all missions on best practices for doing so. There are many forms of donor coordination models, such as working groups, that help enhance information sharing and advance agreement on priorities between donors that are worth evaluating for cyber capacity building purposes.[239]

Objective 15: Streamline the process and improve the timeline for responding to cross-border data requests, in accordance with substantive and procedural protections.

15.1 DOJ, in cooperation with DOS, should strengthen prioritization within the US government for the signing of new executive agreements under the Clarifying Lawful Overseas Use of Data (CLOUD) Act, institute transparency in the process for the negotiation of CLOUD Act agreements, and ensure CLOUD Act agreements are not used as a means for facilitating a backdoor to decryption mandates or other misuses prohibited by the law (Continuous).[240]

Increasingly, digital evidence is critical to the investigation and prosecution of cybercrime and other forms of crime.[241] And that digital evidence is often either located across or controlled by entities that cross international borders. This poses challenges for the United States. Given that so much digital evidence is either controlled by US-based companies and/or physically located within the United States, it poses even greater challenges for foreign governments.[242] US law prohibits US-based companies from disclosing communications content (such as emails or text messages) directly to foreign governments. Instead, foreign governments must make a formal government-to-government request for such data.

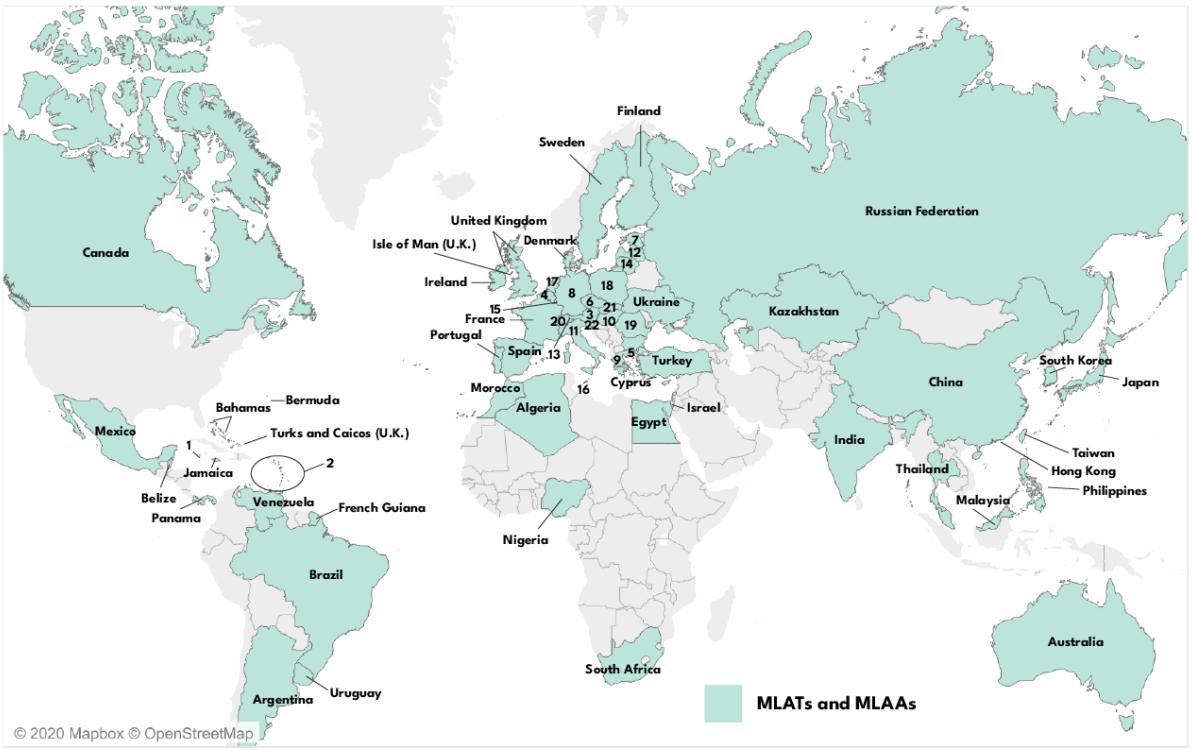
The primary means for making these kinds of data requests is through mutual legal assistance treaties (MLATs) or agreements. However, the United States only has treaties in place with less than half of all countries.[243] And the process, which is managed by DOJ's Office for International

Affairs (OIA), is slow and cumbersome.[244] In FY 2016, DOJ indicated that each OIA attorney was handling three times a manageable caseload.[245] While the "MLAT Reform" program, launched in FY 2016, has helped to reduce the backlog at OIA for MLAT requests, the number of pending cases still remained in the thousands as of DOJ's FY 2019 budget request.[246] DOJ recently noted that "Such delays prompt calls by foreign governments for data localization, trigger foreign demands that [US] Providers produce information directly in response to foreign orders or face criminal penalties, and encourage foreign proposals that [US] Providers be subject to foreign or global data protection regimes."[247]

THIRD WAY

US Mutual Legal Assistance Treaties and Agreements

The United States has negotiated bilateral and multilateral mutual legal assistance treaties (MLATs) and agreements (MLAAs)[1] with foreign governments around the globe, including an MLAT covering the members of the European Union. The following are in force:[2]



1. Cayman Islands (U.K.)	2. Antigua and Barbuda	2. Trinidad and Tobago	5. Bulgaria	13. Liechtenstein	21. Slovakia
2. British Virgin Islands (U.K.)	2. Montserrat (U.K.)	2. St. Vincent & the Grenadines	6. Czech Republic	14. Lithuania	22. Slovenia
2. Anguilla	2. Guadeloupe (France)	2. Curacao (Netherlands)	7. Estonia	15. Luxembourg	
2. St. Martin (France)	2. Dominica	2. Aruba (Netherlands)	8. Germany	16. Malta	
2. Sint Maarten	2. Martinique (France)		9. Greece	17. Netherlands	
2. St. Kitts & Nevis	2. St. Lucia	3. Austria	10. Hungary	18. Poland	
	2. Grenada	4. Belgium	11. Italy	19. Romania	
	2. Barbados		12. Latvia	20. Switzerland	

1 The United States has an MLAA with China, as well as an MLAA between the American Institute in Taiwan and the Taipei Economic and Cultural Representative Office in the United States.

2 The United States has also signed and ratified a number of other multilateral instruments impacting mutual legal assistance.

Sources: United States, Department of State, "Treaties in Force: A List of Treaties and Other International Agreements of the United States in Force on January 1, 2020," 1 Jan. 2020, https://www.state.gov/wp-content/uploads/2020/08/TIF-2020-Full-website-view.pdf. United States, Department of State, "International Narcotics Control Strategy Report: Volume II Money Laundering and Financial Crimes," March 2016, https://2009-2017.state.gov/j/inl/rls/nrcrpt/2016/vol2/253357.htm. Accessed 18 Sept. 2020.

The current backlog for processing requests is not only unsustainable for OIA, it hinders progress in cybercrime investigations globally, which ultimately hurts the United States in bringing to justice the perpetrators of cybercrime. It also reduces the incentive of foreign governments to quickly process requests from the US government for electronic evidence.

The CLOUD Act represents an attempt to alleviate some of this burden, providing a mechanism by which select foreign governments can bypass the mutual legal assistance (MLA) system if they are seeking data about foreigners located outside the United States.[248] Importantly, only those countries that meet certain human rights and rule of law baselines are eligible to enter into these agreements.[249] The US government has only entered into such an agreement with the United Kingdom; it is negotiating another with Australia.[250]

DOJ, in cooperation with DOS, should take several actions to improve the process and procedures for the negotiation of such agreements:

- The Attorney General should make clear the negotiation of CLOUD Act executive agreements is a top priority and ensure that the relevant entities have adequate resources and personnel.
- DOJ should publish CLOUD Act executive agreements, making them accessible to the public. The CLOUD Act requires the Attorney General, in concurrence with the Secretary of State, to certify certain conditions have been made before an executive agreement can be entered into force, and that this certification be published in the Federal Register.[251] No equivalent requirement exists to make the text of these executive agreements public, but there is also nothing in the CLOUD Act that would prohibit the public release of these agreements.[252] In fact, the first agreement with the United Kingdom was made public. The Attorney General should make clear that that will be standard practice moving forward to promote transparency in this process, and Congress should make all necessary changes to the statute to ensure this practice becomes law.
- The Attorney General, in cooperation with the Secretary of State, should put in place effective auditing so that the standards and procedures laid out in the Act are met.
- The agreements should explicitly protect against requests being coupled with decryption mandates or other technical assistance orders.

15.2 DOJ should update guidance on the CLOUD Act, as necessary, to clarify for foreign partners and domestic audiences what the law does and does not do and provide information to those that may misunderstand its intent and scope (Continuous).[253]

In addition to providing updated guidance, DOJ, in cooperation with the DOS, should ensure the network of Resident Legal Advisors, International Computer Hacking and Intellectual Property experts, FBI cyber assistant legal attaches (ALATs), and other personnel deployed overseas to support foreign governments on cybercrime investigations, prosecutions, or capacity building is fully updated on developments with the CLOUD Act and able to provide support and information to foreign partners to understand its purpose and scope, particularly on the powers provided under Part 1 of the law.[254]

15.3 DOJ, in cooperation with DOS, should work to conclude negotiations around the Second Additional Protocol to the Budapest Convention as a means of facilitating more efficient cross-border data sharing while ensuring due process and the protection of civil liberties, and begin work with Congress and the private sector to prepare for implementing legislation (Continuous).

The Budapest Convention's Cybercrime Convention Committee is expected to conclude negotiations on a Second Additional Protocol to the treaty in December 2020. The Second Additional Protocol could make several important changes aimed at facilitating more timely and efficient requests for cross-border data in cybercrime and other criminal investigations.[255]

Given only a limited number of governments can sign CLOUD Act executive agreements, the Second Additional Protocol could be a tremendous incentive for governments to join the Budapest Convention to gain access to the MLA benefits that are being put in place. But strong substantive and procedural protections and civil liberties and human rights safeguards must ensure the Protocol is not misused or abused. The US government should work to conclude negotiations on this Protocol and sign only if such safeguards are adequate in addressing these concerns.[256] Should the US government expect it will sign the Second Additional Protocol, it should begin briefing and consulting key congressional committees, the private sector, and civil society organizations ahead of time concerning its components and possible domestic legislation to facilitate ratification.

15.4 The Attorney General should direct entities within DOJ to adopt recommendations to make the MLAT system more effective and efficient and ensure the annual budget request reflects the resources needed to implement them (101-180 Days).

Even if more CLOUD Act agreements are signed, its rigorous standards mean agreements are only likely to be entered with a small handful of counties. Thus, the challenges to the MLAT system and cross-border data sharing will likely remain in the long-term. DOS's "MLAT Reform" project indicates more resources could have an impact on reducing the remaining backlog and streamlining processes.

There are no shortages of worthwhile recommendations to further reform the MLAT system that deserve consideration. These include increasing US government support to programs aimed at building global capacity on cross-border digital evidence requests and US processes,[257] creating a standardized MLAT request process through electronic forms and online tracking, increasing the number of dedicated personnel working on MLAT requests at OIA, providing OIA with administrative subpoena authority,[258]and ensuring adequate support for translation of outgoing requests. In all these reforms, DOS must uphold civil liberties protections.[259]

The Attorney General should direct DOJ entities with assessing the merit and impact of these proposals and direct them to identify the necessary increased resources and legislative changes required to adopt reforms. Any endorsed reforms and budgetary impacts should be integrated into DOJ's annual budget submission to Congress. Additionally, DOJ, in partnership with DOS, should increase its support for education and training programs for foreign governments on MLA processes.

15.5 DOJ should establish a system to allow for public reporting of MLAT data, including the number of inbound and outbound MLAT requests processed and the average processing time of inbound and outbound requests (181 Days – 1 Year).

No public data currently exists for MLAT requests beyond what has been included in some DOJ Criminal Division budget submissions. However, this data is not standardized across fiscal years, is not always included in every budget request, and contains no granular detail about the scope of governments making such requests and average OIA processing time. This limits transparency for the American public, Members of Congress, and foreign partners wanting to understand the MLAT process. DOS should establish a public reporting system that would be easily accessible to an external audience and request any necessary resources from Congress to implement this system.

15.6 The Attorney General should direct DOJ to provide any necessary additional resources for attaches, legal and cyber advisors, and other personnel placed in foreign missions to meet their mission. DOJ, in cooperation with the FBI and DOS, should evaluate whether decisions are being made as to where to deploy such resources based on a strategic approach and with adequate criteria. DOJ, DOS, and the FBI should work with Congress to authorize and appropriate resources to support increases in personnel as necessary to meet the need (101–180 Days).

DOJ, DOS, FBI, and other government agencies place many personnel in foreign missions to advise on cyber investigations and prosecutions, capacity building, information sharing, MLAs, and other cyber and digital evidence–related priorities.[260] The US Cyberspace Solarium Commission recommends that Congress authorize and fund an additional 12 FBI ALATs.[261] This recommendation deserves consideration, but there are many additional forms of personnel the US government places in foreign missions to boost cyber capacity and advise on cybercrime investigations, prosecutions, and extraditions that also deserve consideration for increased support.

DOJ, in coordination with DOS and FBI, should evaluate whether there are currently adequate resources to support the mission of these personnel in advising and boosting the capacity of foreign criminal justice systems to improve cybercrime enforcement. DOJ and DOS should submit to Congress in their annual budget requests a proposal to increase the number of these personnel where necessary to meet the mission and demand. Further, any such budget request increase should also include an evaluation as to how decisions are being made as to where such personnel are deployed, and all future budgets should include data on the number of these personnel deployed overseas and where they are posted.

Monitoring and Measuring Implementation

Objective 16: Establish processes at lead agencies to measure the implementation of all objectives.

16.1 As part of the implementation of each of these recommendations, the lead department or agency for each should establish a process to set a timeline for implementation and a mechanism to monitor implementation and measure impact (Continuous).

Each of the recommendations in this report include a suggested timeframe for implementation. Recognizing there will be many developments that impact these timeframes, the lead departments and agencies for each of these recommendations should establish a process for establishing a realistic timeframe and a mechanism to hold the entities executing them to account for advancing implementation. Additionally, the lead departments and agencies for each of these recommendations should put in place a mechanism that will allow for an assessment on the impact of each of these measures once they are instituted.

Appendix 1: Summary of Recommendations

Objective	Actions	Timeline	Implementing US Gov. Entity
1. Create and empower a National Cyber Advisor (NCA) position within the Executive Office of the President (EOP).[262]	1.1 The NCA should be located within the EOP.	Day 0	White House
	1.2 The NCA should be a National Security Council (NSC) deputy.		
	1.3 The NCA should not require Senate confirmation.		
	1.4 The NCA should be supported by an Office of the National Cyber Advisor (ONCA).		
	1.5 The ONCA should play a role in planning, organizing, and overseeing strategic disruption of criminal infrastructures.		
	1.6 The ONCA should be allotted a staff of 25–30 people.		
	1.7 The ONCA should have dedicated funding within the EOP budget.		
	1.8 The ONCA should concurrently review federal cybersecurity budgets with the Office of Management and Budget (OMB).		
	1.9 The ONCA should be transparent about its interaction with the private sector.		
	1.10 The ONCA should prioritize transparency by publishing an annual report.		
2. Enable the ONCA to coordinate with federal agencies to identify, resolve, and develop proposals to improve interagency processes and federal partnerships with external stakeholders to close the cyber enforcement gap	2.1 The ONCA should lead a temporary, intergovernmental Cybercrime Working Group that consists of the Departments of Justice (DOJ), Homeland Security (DHS), State (DOS), Treasury, and the Federal Bureau of Investigation (FBI), US Secret Service (USSS), and other relevant federal entities to assess and develop interagency policies and legislative proposals on cybercrime and cyber enforcement, particularly in areas where cross-agency coordination and cooperation is required, and to coordinate with the private sector and SLTT partners when necessary.	0–100 Days	ONCA

3. Introduce legislation that permanently places the Vulnerabilities Equities Process (VEP) under the purview of the ONCA and increases the transparency of the VEP.	3.1 The NCA should work with Congress to develop legislation establishing a permanent Equities Review Board (ERB) within the ONCA.	0–100 Days	White House (with Congress)
	3.2 In this legislation, Congress should establish a permanent VEP Director position to lead the ERB, supported by an Executive Secretariat.		
	3.3 Congress should require all US government agencies to timely submit all known vulnerabilities for review by the ERB.		
	3.4 Congress should require the VEP Executive Secretariat to publish an annual report about the ERB.		
	3.5 The VEP Director should clarify that the VEP applies to both purchased and internally discovered vulnerabilities.		
	3.6 The VEP Director should ensure that voting power within the ERB is distributed equitably and should clarify the process to resolve disagreements.		
	3.7 The VEP Director should establish procedures for conducting regular reviews of the ERB.		
4. Update the US government's approach to cyber threat intelligence collection and sharing around cybercrime.	4.1 The Office of the Director of National Intelligence (ODNI) and the ONCA should create a joint working group to identify intelligence collection gaps on cybercrime and propose ways to close those gaps.	0–100 Days	ODNI and ONCA
	4.2 The ONCA should integrate functional intelligence collection priorities related to cybercrime into regional intelligence priorities.	101–180 Days	ONCA
	4.3 The ONCA should work with the Intelligence Community (IC) to update US government cyber threat intelligence analysis to produce adversary playbooks that describe cyber threat actors' typical tactics, techniques, and procedures.	Day 0	ONCA
	4.4 The Cybercrime Working Group should enhance effective intergovernmental and public information sharing about cyber threat vectors, including those related to cybercrime.	0–100 Days	Cybercrime Working Group
	4.5 The Director of National Intelligence (DNI) shall prepare a National Intelligence Estimate (NIE) on the relationship between criminal cyber actors and nation-states.	Day 0	ODNI
5. Develop a dedicated strategic approach to cyber enforcement as part of a US national cyber strategy.	5.1 The NCA should target a specific amount by which to reduce the economic impact of cybercrime by 2024.	101–180 Days	ONCA
	5.2 ONCA staff should consult the private sector and civil society groups to identify barriers to the reduction of the economic impact of cybercrime.	101–180 Days	
	5.3 The NCA should work through an interagency process to immediately draft a cybercrime addendum to the 2018 National Cyber Strategy and eventually strengthen the cybercrime components of a new or updated national cyber strategy.	101–180 Days	

6. Identify and clarify roles and responsibilities among federal and state, local, tribal, and territorial (SLTT) criminal justice agencies to strengthen institutionalized processes and relationships with public, private, and international partners to improve cybercrime investigations and prosecutions.	6.1 The Cybercrime Working Group should clearly delineate cyber enforcement roles and responsibilities within federal entities, and between federal and SLTT, private, and international partners to create more effective, interagency coordination.	101–180 Days	Cybercrime Working Group
7. Increase prioritization of cybercrime among federal, SLTT, and private sector stakeholders and direct federal resources to federal and SLTT agencies that are commensurate with its prevalence and impact.	7.1 OMB and the ONCA should review all federal departments and agencies with cyber enforcement missions to create a comprehensive cyber enforcement budget proposal for the President's Budget Request for FY 2023 or FY 2024.	101–180 Days	OMB and ONCA
	7.2 The ONCA should develop a plan to attend and hold a series of forums and workshops with SLTT and private sector participants to discuss challenges of cyber enforcement and areas to improve partnerships.	0–100 Days	ONCA
8. Develop uniform metrics to inform and improve data reporting, victim response, and national data collection for federal and SLTT law enforcement.	8.1 The ONCA should consult with relevant federal departments and agencies to develop uniform metrics to evaluate the federal government's efforts to reduce cybercrime and to inform data collection efforts.	101–180 Days	ONCA
	8.2 DOJ and FBI should develop policies and legislative proposals to expand cybercrime categories in the National Incident-Based Reporting System (NIBRS), further spur the uptake of NIBRS, and explore other initiatives to improve data reporting.	1 Year+	DOJ and FBI
	8.3 To improve law enforcement's response to victims, the Cybercrime Working Group should develop proposals that improve cybercrime reporting among public and private victims and the assistance awarded to them.	1 Year+	Cybercrime Working Group
9. Strengthen federal and SLTT law enforcement's ability to share investigative information related to cybercrime.	9.1 The Cybercrime Working Group should develop policies and propose additional funding to strengthen existing information sharing mechanisms to enable investigations by criminal justice agencies.	1 Year+	Cybercrime Working Group

10. Improve the digital evidence forensic capacity and capability of federal and SLTT criminal justice agencies by reforming recruitment, training, and retention practices.	10.1 The Office of Personnel Management (OPM) and OMB should issue a memorandum that outlines policy proposals and propose funds for FY 2023 and/or FY 2024 to improve recruitment practices for federal law enforcement agencies regarding cyber enforcement personnel.	101–180 Days	OPM and OMB
	10.2 In their updated memorandum, OPM and OMB should include policy proposals and propose funds for FY 2023 and/or FY 2024 to expand training opportunities for federal and SLTT law enforcement and other criminal justice agencies and retain those employees once trained.	101–180 Days	OPM and OMB
	10.3 The ONCA should work with Congress to develop legislation to ensure that federal and SLTT criminal justice agencies have access to technical assistance to examine digital evidence.	0–100 Days	ONCA
	10.4 DOJ should develop policies and request sufficient funding so that federal and SLTT criminal justice agencies have access to technical assistance to examine digital evidence.	0–100 Days	DOJ
11. Assess the needs, resources, and capacity of SLTT criminal justice agencies and federal–state collaborative organizations to address cybercrime.	11.1 DOJ should coordinate with DHS to assess the gap between the needs of SLTT criminal justice agencies and their capabilities and capacities.	0–100 Days	DOJ and DHS
	11.2 DOJ should determine how many localities are using the Edward Byrne Memorial Justice Assistance Grant (JAG) program for cybercrime initiatives, how much these localities have received for these initiatives, how the program could be used to promote SLTT cyber enforcement, and whether other grant programs should be expanded.	0–100 Days	DOJ
	11.3 DOJ and DHS should identify and recommend proposals on how to improve and expand federal and SLTT cybercrime task forces.	0–100 Days	DOJ and DHS
12. Establish a new structure in the Department of State (DOS) to ensure a well-resourced single point of high-level leadership for all cyber diplomacy matters, backed by an architecture that allows for other bureaus advancing policy and programming on cybercrime to effectively coordinate.	12.1 The Secretary of State should establish an Office of International Cyberspace Policy at DOS with the head of Office having the rank and status of Ambassador and ensure this Office is supported with the adequate funding and personnel to fulfill its mandate.[263]	0–100 Days	DOS
	12.2 The White House should work with Congress to codify the Office of International Cyberspace Policy at DOS.	0–100 Days	White House

13. Identify a set of diplomatic tools and policy options to boost international cooperation in cybercrime investigations and address governments that are systematically uncooperative.	13.1 DOS, in coordination with the White House and all relevant departments and agencies in the US government, including the IC, should draft a new US global cyber engagement strategy through an interagency process. This strategy should be updated every four years and inform the development of a national cyber strategy by the White House.	1 Year+	DOS
	13.2 Once a new global cyber engagement strategy is issued, all regional DOS bureaus and USAID should be required to update or draft new regional cyber strategies to align with the newly established goals and objectives.	1 Year+	DOS
	13.3 DOS should include cybercrime and other cyber priorities in other key review and strategic planning documents for the Department and USAID. This should include any and all future Quadrennial Diplomacy and Development Reviews (QDDR).	1 Year+	DOS
	13.4 DOS should enhance its training and awareness raising on cybercrime for policy officers at posts, encourage posts to add cybercrime as a standing item to Law Enforcement Working Groups, identify additional Department-wide training opportunities to enhance training and awareness on cybercrime, and dedicate time at annual Chiefs of Mission meetings for updates on cyber developments.	101–180 Days	DOS
	13.5 The Department of Treasury, in coordination with all relevant departments and agencies including the IC, should undertake an inter-agency assessment of the effectiveness of all existing cyber-related sanctions in halting or reducing malicious cyber activity.	101–180 Days	Treasury Department
	13.6 DOS, in cooperation with the Department of Treasury, should increase support to non-governmental research institutions to conduct regular, independent assessments of the effectiveness of cyber sanctions and propose recommendations to improve the US's cyber sanctions regime.	1 Year+	DOS
	13.7 Should the United States choose to participate in negotiations on a new global cybercrime convention, it should develop a strategy for engagement and ensure the process is transparent, inclusive, and safeguards human rights.	1 Year+	White House

14. Identify a group of countries where the US government is not receiving timely assistance in cybercrime investigations and develop programs to support their criminal justice capacity building needs—including operational support, policy development, and harmonization of laws—to boost cooperation.	14.1 As part of the development of a new global cyber engagement strategy, DOS should work in cooperation with USAID, DOJ, FBI, the IC, and all other relevant federal entities to develop an assessment, monitoring, and evaluation (AM&E) framework for all cyber foreign capacity building programs funded through annual foreign assistance resources. This AM&E framework should inform and ultimately be integrated into a broader DOS security sector assistance AM&E framework.	181 Days–1 Year	DOS
	14.2 The DOS Office of International Cyberspace Policy, in partnership with the International Narcotics and Law Enforcement Bureau (INL) and relevant federal entities, should lead a process that identifies a target number of countries where the US government is not receiving timely assistance in cybercrime investigations and it is determined that increased support to their cyber capacity building needs may have an impact.	1 Year+	
	14.3 DOS should take steps to establish regional and/or in-country donor coordination mechanisms on cyber capacity building to overcome the duplication in funding that has been observed from donor governments.	1 Year+	
15. Streamline the process and improve the timeline for responding to cross-border data requests, in accordance with substantive and procedural protections.	15.1 DOJ, in cooperation with DOS, should strengthen prioritization within the US government for the signing of new executive agreements under the "Clarifying Lawful Overseas Use of Data Act" (CLOUD), institute transparency in the process for the negotiation of CLOUD Act agreements, and ensure CLOUD Act agreements are not used as a means for facilitating a backdoor to decryption mandates or other misuses prohibited by the law.	Continuous	DOJ and DOS
	15.2 DOJ should update guidance on the CLOUD Act, as necessary, to clarify for foreign partners and domestic audiences what the law does and does not do and provide information to those that may misunderstand its intent and scope.	Continuous	DOJ
	15.3 DOJ, in cooperation with DOS, should work to conclude negotiations around the Second Additional Protocol to the Budapest Convention as a means of facilitating more efficient cross-border data sharing while ensuring due process and the protection of civil liberties, and begin work with Congress and the private sector to prepare for implementing legislation.	Continuous	DOJ
	15.4 The Attorney General should direct entities within DOJ to adopt recommendations to make the MLAT system more effective and efficient and ensure the annual budget request reflects the resources needed to implement them.	101–180 Days	DOJ

	15.5 DOJ should establish a system to allow for public reporting of MLAT data, including the number of inbound and outbound MLAT requests processed and the average processing time of inbound and outbound requests.	181 Days–1 Year	DOJ
	15.6 The Attorney General should direct DOJ to provide any necessary additional resources for attaches, legal and cyber advisors, and other personnel placed in foreign missions to meet their mission. DOJ, in cooperation with the FBI and DOS, should evaluate whether decisions are being made as to where to deploy such resources based on a strategic approach and with adequate criteria. DOJ, DOS, and the FBI should work with Congress to authorize and appropriate resources to support increases in personnel as necessary to meet the need.	101–180 days	DOJ
16. Establish processes at lead agencies to measure the implementation of all objectives	16.1 As part of the implementation of each of these recommendations, the lead department or agency for each should establish a process to set a timeline for implementation and a mechanism to monitor implementation and measure impact.	Continuous	All lead departments and agencies

Appendix 2: Abbreviations

Abbreviation	Meaning
ALATs	Cyber Assistant Legal Attachés
AM&E	Assessment, Monitoring, and Evaluation
BJA	Bureau of Justice Assistance
BJS	Bureau of Justice Statistics
Budapest Convention	Convention on Cybercrime of the Council of Europe
CJIS APB	Criminal Justice Information Services Advisory Policy Board
CLOUD Act	Clarifying Lawful Overseas Use of Data Act
DHS	Department of Homeland Security
DNI	Director of National Intelligence
DOJ	Department of Justice
DOS	Department of State
EOP	Executive Office of the President
ERB	Equities Review Board
EU	European Union
FBI	Federal Bureau of Investigation
FCWAA	Federal Cybersecurity Workforce Assessment Act of 2015
FFRDC	Federally Funded Research and Development Centers
FTC	Federal Trade Commission
FY	Fiscal Year
IC	Intelligence Community

IC3	Internet Crime Complaint Center
ICT	Information and Communication Technology
INL	Bureau of International Narcotics and Law Enforcement Affairs
IP	Intellectual Property
IPC	Interagency policy committee
IPR	Intellectual Property Rights
ISACs	Information Sharing and Analysis Centers
JAG	Edward Byrne Memorial Justice Assistance Grant
MLA	Mutual Legal Assistance
MLATs	Mutual Legal Assistance Treaties
NATO	North Atlantic Treaty Organization
NCA	National Cyber Advisor
NCFI	National Computer Forensic Institute
NCFTA	National Cyber-Forensics and Training Alliance
NCIJTF	National Cyber Investigative Joint Task Force
NDCAC	National Domestic Communications Assistance Center
NEC	National Economic Council
NGOs	Nongovernment Organizations
NIBRS	National Incident-Based Reporting System
NICE	National Institute for Cybersecurity Education
NIE	National Intelligence Estimate
NIST	National Institute of Standards and Technology

NSA	National Security Agency
NSC	National Security Council
NSF	National Science Foundation
NSPD	National Security Presidential Directive
NW3C	National White Collar Crime Center
ODNI	Office of the Director of National Intelligence
OIA	Office for International Affairs
OMB	Office of Management and Budget
ONCA	Office of the National Cyber Advisor
OPM	Office of Personnel Management
OVC	Office for Victims of Crime
QDDR	Quadrennial Diplomacy and Development Reviews
SCCs	Sector Coordinating Councils
SLTT	State, Local, Tribal, and Territorial
TTPs	Tactics, Techniques, and Procedures
UCR	Uniform Crime Reporting
UN	United Nations
USAID	US Agency for International Development
USSS	US Secret Service
VEP	Vulnerabilities Equities Process

ENDNOTES

1 There is no global consensus on the definition of the term "cybercrime." The Council of Europe's 2001 Convention on Cybercrime (also known as the Budapest Convention), which the United States ratified in 2006, defines acts of cybercrime (as opposed to perpetrators) as "action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data." Council of Europe. Convention on Cybercrime, 23 Nov. 2001, p. 2 (Preamble). www.refworld.org/docid/47fdfb202.html. Accessed 18 October 2020. The Convention contains four categories of criminal offenses: (1) offenses against the confidentiality, integrity, and availability of computer data and systems, (2) computer-related offenses, (3) content-related offenses, and (4) offenses related to infringements of copyright and related rights. This roadmap focuses on those offenses against the confidentiality, integrity, and availability of computer data and systems and not on content-related offences, such as those related to child pornography, terrorism propaganda, and hate speech.

2 Newman, Lily Hay. "Atlanta Spent $2.6M to Recover From a $52,000 Ransomware Scare." Wired, 23 Apr. 2018, www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/. Accessed 17 Oct. 2020.; Fernandez, Manny, et al. "Ransomware Attacks Hits 22 Texas Towns, Authorities Say." The New York Times, 20 Aug. 2019, www.nytimes.com/2019/08/20/us/texas-ransomware.html. Accessed 17 Oct. 2020.

3 Fazzini, Kate. "Here's how online scammers prey on older Americans, and what they should know to fight back." CNBC, 23 Nov. 2019, www.cnbc.com/2019/11/23/new-research-pinpoints-how-elderly-people-are-targeted-in-online-scams.html. Accessed 17 Oct. 2020.

4 US Department of Homeland Security. "Commodification of Cyber Capabilities: A Grand Cyber Arms Bazaar." 2019, www.dhs.gov/sites/default/files/publications/ia/ia_geopolitical-impact-cyber-threats-nation-state-actors.pdf. Accessed 17 Oct. 2020.

5 Kass, DH. "FBI: COVID-19 Cyberattacks spike 400% in Pandemic." MSSP Alert, https://www.msspalert.com/cybersecurity-news/fbi-covid-19-cyberattacks-spike-400-in-pandemic/. Accessed 17 Oct. 2020.

6 Miller, Maggie. "Senior official estimates $30 billion in stimulus funds will be stolen through coronavirus scams." The Hill, 9 June 2020, https://thehill.com/policy/cybersecurity/501936-senior-official-estimates-30-billion-in-stimulus-funds-will-be-stolen?utm_campaign=wp_the_cybersecurity_202&utm_medium=email&utm_source=newsletter&wpisrc=nl_cybersecurity202. Accessed 17 Oct. 2020.

7 Kalra, Jaspreet. "UCSF Hospital Paid $1.14M in Bitcoin After Ransomware Attack." Coindesk, 30 June 2020, www.coindesk.com/ucsf-hospital-paid-1-14m-in-bitcoin-after-ransomware-attack. Accessed 17 Oct. 2020.

8 Eddy, Melissa and Perlroth, Nicole. "Cyber Attack Suspected in German Woman's Death." New York Times, 18 Sept. 2020. https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html. Accessed 18 Oct. 2020.

9 "WHO reports fivefold increase in cyber attacks, urges vigilance." Press Release, The World Health Organization, 23 Apr. 2020, https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance#:~:text=Since%20the%20start%20of%20the,targeting%20the%20public%20at%20large. Accessed 17 Oct. 2020.

10 Reinhart, RJ. "One in Four Americans Have Experienced Cybercrime." Gallup, 11 Dec. 2018, news.gallup.com/poll/245336/one-four-americans-experienced-cybercrime.aspx. Accessed 17 Oct. 2020.

11 Decker, Eileen. "Full Count?: Crime Rate Swings, Cybercrime Misses and Why We Don't Really Know the Score." Journal of National Security Law & Policy, Vol. 10:583, May 2020, pp. 583-584. jnslp.com/wp-content/uploads/2020/05/Crime-Rate-Swings-Cybercrime-Misses.pdf. Accessed 17 Oct. 2020.

12 Decker, Eileen. "Full Count?: Crime Rate Swings, Cybercrime Misses and Why We Don't Really Know the Score." Journal of National Security Law & Policy, Vol. 10:583, May 2020, pp. 583-584. jnslp.com/wp-content/uploads/2020/05/Crime-Rate-Swings-Cybercrime-Misses.pdf. Accessed 17 Oct. 2020.

13 US White House, The Council of Economic Advisers. The Cost of Malicious Cyber Activity to the U.S. Economy. February 2018, p. 36. www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf. Accessed 17 Oct. 2020.

14 Bissell, Kelly, et al. "2019 Cost of Cybercrime." Accenture, 6 Mar. 2019, p. 11. https://www.accenture.com/us-en/insights/security/cost-cybercrime-study. Accessed 17 Oct. 2020.

15 Ablon, Lillian. "Data Thieves: The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data." Rand, Testimony presented before the House Financial Services Committee, Subcommittee on Terrorism and Illicit Finance, 15 Mar. 2018, www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT490/RAND_CT490.pdf. Accessed 17 Oct. 2020.

16 US Department of Homeland Security. "Commodification of Cyber Capabilities: A Grand Cyber Arms Bazaar." 2019, pp. 4-5. www.dhs.gov/sites/default/files/publications/ia/ia_geopolitical-impact-cyber-threats-nation-state-actors.pdf. Accessed 17 Oct. 2020; Healey, Jason. "Beyond Attribution: Seeking National Responsibility for Cyber Attacks." The Atlantic Council, 22 Feb. 2012, www.atlanticcouncil.org/wp-content/uploads/2012/02/022212_ACUS_NatlResponsibilityCyber.PDF. Accessed 17 Oct. 2020.

17 Nakashima, Ellen and Barrett, Devlin. "U.S. accuses China of sponsoring criminal hackers targeting coronavirus vaccine research." The Washington Post, 21 July 2020, www.washingtonpost.com/national-security/us-china-covid-19-vaccine-research/2020/07/21/8b6ca0c0-cb58-11ea-91f1-28aca4d833a0_story.html. Accessed 17 Oct. 2020.

18 Eoyang, Mieke, et al. "To Catch a Hacker: Toward a comprehensive strategy to identify, pursue, and punish malicious cyber actors." Third Way, 29 Oct. 2018, www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors. Accessed 17 Oct. 2020.

19 Eoyang, Mieke, et al. "To Catch a Hacker: Toward a comprehensive strategy to identify, pursue, and punish malicious cyber actors." Third Way, 29 Oct 2018, www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors. Accessed 17 Oct. 2020.

20 Peters, Allison and Jordan, Amy. "Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime." Journal of National Security Law & Policy, Vol. 10:583, May 2020, p. 490. jnslp.com/wp-content/uploads/2020/05/Countering-the-Cyber-Enforcement-Gap.pdf. Accessed 17 Oct. 2020.

21 Mehta, Ishan. "Poll Shows Voters Want Next President to Make Reducing Cybercrime a Top Priority." Third Way, 1 Oct. 2019, www.thirdway.org/blog/poll-shows-voters-want-next-president-to-make-reducing-cybercrime-a-top-priority. Accessed 17 Oct. 2020.

22 "Crimes Americans Worry About Most in 2019." Statista, 11 Dec. 2019. www.statista.com/statistics/339735/crime-worries-in-the-united-states/. Accessed 17 Oct. 2020.

23 Smeltz, Dina, et al. "Rejecting Retreat: Americans Support US Engagement in Global Affairs." The Chicago Council on Global Affairs, 9 Sept. 2019, p. 34. www.thechicagocouncil.org/sites/default/files/report_ccs19_rejecting-retreat_20190909.pdf. Accessed 17 Oct. 2020; Poushter, Jacob and Fagan, Moira. "Americans See Spread of Disease as Top International Threat, Along with Terrorism, Nuclear Weapons, Cyberattacks." Pew Research Center, 13 Apr. 2020, www.pewresearch.org/global/2020/04/13/americans-see-spread-of-disease-as-top-international-threat-along-with-terrorism-nuclear-weapons-cyberattacks/. Accessed 17 Oct. 2020.

24 Pougiales, Ryan and Erickson, Lanae. "Voters Views' about Technology and Public Policy." Third Way, 24 Apr. 2020. www.thirdway.org/memo/voters-views-about-technology-and-public-policy. Accessed 17 Oct. 2020.

25 Eoyang, Mieke, et al. "To Catch a Hacker: Toward a comprehensive strategy to identify, pursue, and punish malicious cyber actors." Third Way, 29 Oct. 2018. www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors. Accessed 17 Oct. 2020.

26 Dorfman, Zach. Et al. "Exclusive: Secret Trump order gives CIA more powers to launch cyberattacks." Yahoo News, 15 July 2020. https://news.yahoo.com/secret-trump-order-gives-cia-more-powers-to-launch-cyberattacks-090015219.html. Accessed 17 Oct. 2020.

27 Eoyang, Mieke and Keitner, Chimene. "Cybercrime vs. Cyberwar: Paradigms for Addressing Malicious Cyber Activity." Journal of National Security Law and Policy, 4 Mar. 2020. papers.ssrn.com/sol3/papers.cfm?abstract_id=3599588. Accessed 17 Oct. 2020.

28 Eoyang, Mieke and Keitner, Chimene. "Cybercrime vs. Cyberwar: Paradigms for Addressing Malicious Cyber Activity." Journal of National Security Law and Policy, 4 Mar. 2020, papers.ssrn.com/sol3/papers.cfm?abstract_id=3599588. Accessed 17 Oct. 2020.

29 Hinck, Garrett and Maurer, Tim. "Persistent Enforcement: Criminal Charges as a Response to Nation-State Malicious Cyber Activity." Journal of National Security Law and Policy, Vol. 10:525, 23 Jan. 2020, jnslp.com/wp-content/uploads/2020/05/Criminal-Charges-as-a-Response-to-Nation-State-Malicious-Cyber-Activity.pdf. Accessed 17 Oct. 2020.

30 In May 2018, the role of "cyber coordinator" was eliminated, with lower-level National Security Council staff assuming the roles and responsibilities that had resided in a single senior official since 1998. Clinton White House. "The Clinton Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63." Clinton White House Archives, May 1998, clintonwhitehouse4.archives.gov/textonly/WH/EOP/NSC/html/documents/NSCDoc3.html. Accessed 17 Oct. 2020; Geller, Eric. "White House eliminates top cyber adviser post." Politico, 15 May 2018, www.politico.com/story/2018/05/15/white-house-eliminates-cyber-adviser-post-542916. Accessed 17 Oct. 2020.

31 See, e.g., Sabin, Sam. "In Fight Against COVID-19 Scam Sites, Lawmakers Push for Domain Name Ownership Records, More Accountability." Morning Consult, 2 June 2020, morningconsult.com/2020/06/02/whois-database-public-domain-name-ownership-coronavirus-scams/. Accessed 17 Oct. 2020.

32 Joyce, Rob. "Improving and Making the Vulnerability Equities Process Transparent is the Right Thing to Do." WhiteHouse.gov, 15 Nov. 2017, www.whitehouse.gov/articles/improving-making-vulnerability-equities-process-transparent-right-thing/. Accessed 17 Oct. 2020.; Schwartz, Ari. Et al. "Government's Role in Vulnerability Disclosure: Creating a Permanent and Accountable Vulnerability Equities Process." Belfer Center for Science and International Affairs, June 2016. https://www.belfercenter.org/sites/default/files/legacy/files/vulnerability-disclosure-web-final3.pdf. Accessed 17 Oct. 2020.

33 Wexler, Chuck. "New National Commitment Required: The Changing Nature of Crime and Criminal Investigations." Police Executive Research Forum, Jan. 2018, p. 14. www.policeforum.org/assets/ChangingNatureofCrime.pdf. Accessed 17 Oct. 2020.

34 US Security Exchange Commission. "Commission Statement and Guidance on Public Company Cybersecurity Disclosures." SEC, 17 CFR Parts 229 and 249, 26 Feb. 2018, pp. 3-4. www.sec.gov/rules/interp/2018/33-10459.pdf. Accessed 17 Oct. 2020.

35 Mehta, Ishan. "The Need for Better Metrics on Cybercrime." Third Way, 1 Oct 2019, www.thirdway.org/memo/the-need-for-better-metrics-on-cybercrime. Accessed 17 Oct. 2020.

36 Carter, William, et al. "Low-Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge." Center for Strategic and International Studies, July 2018, p.12. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/180725_Carter_DigitalEvidence.pdf?tAGR_DvxRdp0RspiGYNGcGKTUjrGY3rN. Accessed 17 Oct. 2020.

37 Carter, William, et al. "Low-Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge." Center for Strategic and International Studies, 2018 July, p.12. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/180725_Carter_DigitalEvidence.pdf?tAGR_DvxRdp0RspiGYNGcGKTUjrGY3rN. Accessed 17 Oct. 2020.

38 US Department of Commerce and US Department of Homeland Security. "A Report to the President On Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future." 30 May 2018. www.nist.gov/system/files/

documents/2018/07/24/eo_wf_report_to_potus.pdf. Accessed 17 Oct. 2020; Gardiner, Christine. "How Educated Should Police Be?" National Police Foundation, https://www.policefoundation.org/study-examines-higher-education-in-policing/#:~:text=About%20one%20third%20(30.2%20percent,percent%20have%20a%20graduate%20degree. Accessed 17 Oct. 2020.

39 "Cybersecurity Supply/Demand Heat Map." CyberSeek, www.cyberseek.org/heatmap.html. Accessed 17 Oct. 2020.

40 Garcia, Michael and Hindocha, Anisha. "Where Are We Now? Examining the Trump Administration's Efforts to Combat Cybercrime." Third Way, 22 June 2020, www.thirdway.org/report/where-are-we-now-examining-the-trump-administrations-efforts-to-combat-cybercrime. Accessed 17 Oct. 2020.

41 The National Domestic Communications Center Executive Advisory Board. "Report to the Attorney General." National Domestic Communications Assistance Center, Federal Bureau of Investigation, July 2019, p.7. https://ndcac.fbi.gov/file-repository/second-report-to-ag-20190716.pdf/view. Accessed 17 Oct 2020.

42 US Department of Justice, Federal Bureau of Investigation. "Working at FBI: Diversity." FBI, www.fbijobs.gov/working-at-FBI/diversity. Accessed 17 Oct. 2020; Department of Homeland Security, Equal Employment Opportunity and Diversity Division. "EEO Diversity Management." DHS, www.dhs.gov/dhs-diversity-planning. Accessed 17 Oct. 2020.

43 Rock, David and Grant, Heidi. "Why Diverse Teams Are Smarter." Harvard Business Review, 4 Nov. 2016, hbr.org/2016/11/why-diverse-teams-are-smarter. Accessed 17 Oct. 2020.

44 US Department of Commerce and US Department of Homeland Security. "A Report to the President On Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future." 30 May 2018, www.nist.gov/system/files/documents/2018/07/24/eo_wf_report_to_potus.pdf. Accessed 17 Oct. 2020; US Cyberspace Solarium Commission. "Growing a Stronger Federal Cyber Workforce." CSC White Paper #3, Sept. 2020, drive.google.com/file/d/1WGNHpVmf4X12zv6DWuq9V4GtKF3jz92e/view. Accessed 17 Oct. 2020.

45 US Government Accountability Office. "Cybersecurity: Clarity of Leadership Urgently Needed to Fully Implement the National Strategy." Sept. 2020. www.gao.gov/assets/710/709555.pdf?utm_campaign=wp_the_cybersecurity_202&utm_medium=email&utm_source=newsletter&wpisrc=nl_cybersecurity202. Accessed 17 Oct. 2020.

46 Peters, Allison and Jordan, Amy. "Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime." Journal of National Security Law & Policy, Vol. 10:583, May 2020, p. 520. jnslp.com/wp-content/uploads/2020/05/Countering-the-Cyber-Enforcement-Gap.pdf. Accessed 17 Oct. 2020.

47 "Freedom on the Net 2019: The Crisis of Social Media." Freedom House, 4 Nov. 2019, https://freedomhouse.org/report/freedom-net/2019/crisis-social-media. Accessed 17 Oct. 2020.

48 Healey, Jason. "Beyond Attribution: Seeking National Responsibility for Cyber Attacks." The Atlantic Council. 22 Feb. 2012, www.atlanticcouncil.org/wp-content/uploads/2012/02/022212_ACUS_NatlResponsibilityCyber.PDF. Accessed 17 Oct. 2020; Eoyang, Mieke, et al. "To Catch a Hacker: Toward a comprehensive strategy to identify, pursue, and punish malicious cyber actors." Third Way, 29 Oct. 2018, www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors. Accessed 17 Oct. 2020.

49 See, e.g., Sanger, David E. "U.S. Declines to Sign Declaration Discouraging Use of Cyberattacks." New York Times, 12 Nov. 2018, www.nytimes.com/2018/11/12/us/politics/us-cyberattacks-declaration.html. Accessed 17 Oct. 2020.

50 Council of Europe. "Budapest Convention and related standards." www.coe.int/en/web/cybercrime/the-budapest-convention. Accessed 18 Oct. 2020.

51 United States, Congress, Government Accountability Office. "Department of State, Integrated Action Plan Could Enhance Efforts to Reduce Persistent Overseas Foreign Service Vacancies." GAO, Mar. 2019, www.gao.gov/assets/700/697281.pdf. Accessed 17 Oct. 2020; Gramer, Robbie and Groll, Elias. "Can State's New Cyber Bureau Hack It?" Foreign Policy, 18 Jan. 2019, foreignpolicy.com/2019/01/18/state-

department-cyber-security-cyber-threats-russia-china-diplomacy-capitol-hill-lawmakers-pompeo/. Accessed 17 Oct. 2020.

52 Hakmeh, Joyce and Peters, Allison. "A New UN Cybercrime Treaty? The Way Forward for Supporters of an Open, Free, and Secure Internet." The Council on Foreign Relations, 13 Jan. 2020, www.cfr.org/blog/new-un-cybercrime-treaty-way-forward-supporters-open-free-and-secure-internet. Accessed 17 Oct. 2020.

53 See for example, passage of the 2018 Clarifying Lawful Overseas Use of Data (CLOUD) Act (P.L. 115-141, Division V). United States, Congress, House. Consolidated Appropriations Act of 2018. Congress.gov, www.congress.gov/115/plaws/publ141/PLAW-115publ141.pdf, 115th Congress, 2nd session, P.L. 115-141, div. V, passed 23 Mar. 2018.

54 At the time of writing, Congress has pending legislation to create a National Cyber Director (NCD) that would perform similar, but not all, duties recommended in this report. The legislation authorizes this position at the Director level, but for the purposes of this publication the National Cyber Advisor will be used to refer to this position. United States, Congress, House, William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021. Congress.gov, www.congress.gov/116/bills/hr6395/BILLS-116hr6395pcs.pdf, 116th Congress, 2nd session, H.R. 6395, Section 1132, 5. Accessed 17 Oct. 2020.

55 There are six categories of timelines for when each recommendation should be implemented: Day 0 (the first week of an Administration), 0-100 Days, 101-180 Days, 181 Days-1 Year, 1 Year+, and continuous implementation.

56 Hinck, Garrett and Maurer, Tim. "Persistent Enforcement: Criminal Charges as a Response to Nation-State Malicious Cyber Activity." The Journal of National Security Law and Policy, 23 Jan. 2020, jnslp.com/2020/01/23/persistent-enforcement-criminal-charges-as-a-response-to-nation-state-malicious-cyber-activity/. Accessed 17 Oct. 2020.

57 This recommendation diverges from the US Cyberspace Solarium Commissions recommendation for a 50-person staff. Since the office's primary mission would be coordination, 50 people is more than needed. Further, context, an office of 50 people in the White House seems overly large. US Cyberspace Solarium Commission. "CSC Final Report." March 2020, p.38. drive.google.com/file/d/1ryMCIL__dZ30QyjFqFkkf10MxIXJGT4yv/view. Accessed 17 Oct. 2020.

58 US White House. "Presidential Policy Directive—United States Cyber Incident Coordination." White House Obama Archives, 26 July 2016, obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident. Accessed 17 Oct. 2020.

59 This senior role will help to ensure coordination among economic, law enforcement, and national security efforts.

60 Maurer, Tim and Nelson, Arthur. "An International Strategy to Better Protect the Financial System against Cyber Threats (2021-2024)," Carnegie Endowment for International Peace, forthcoming, see carnegieendowment.org/specialprojects/fincyber/about/. Accessed 17 Oct. 2020.

61 US Office of Personnel Management. "Policy, Data, Oversight: Hiring Information." OPM, www.opm.gov/policy-data-oversight/hiring-information/intergovernment-personnel-act/. Accessed 17 Oct. 2020.

62 Maurer, Tim and Nelson, Arthur. "An International Strategy to Better Protect the Financial System against Cyber Threats (2021-2024)," Carnegie Endowment for International Peace, forthcoming, see carnegieendowment.org/specialprojects/fincyber/about/. Accessed 17 Oct. 2020; "Partnership against Cybercrime," World Economic Forum, https://www.weforum.org/projects/partnership-against-cybercime. Accessed 20 Oct. 2020.

63 The Obama Administration regularly published all visitor logs. If the White House were to publish those logs, the ONCA could reference them in the annual report as an acceptable alternative mechanism to track the ONCA's interactions with the private sector.

64 This working group should not have any operational authority. Depending on how the working group is created, structured, and its remit, it may be subject to the Federal Advisory Committee Act. See US General Services Administration. "The Federal Advisory Committee Act." GSA, www.gsa.gov/policy-

regulations/policy/federal-advisory-committee-management/legislation-and-regulations/the-federal-advisory-committee-act. Accessed 17 Oct. 2020.

65 Joyce, Rob. "Improving and Making the Vulnerability Equities Process Transparent is the Right Thing to Do." WhiteHouse.gov, 15 Nov. 2017, www.whitehouse.gov/articles/improving-making-vulnerability-equities-process-transparent-right-thing/. Accessed 17 Oct. 2020.

66 US White House. "Vulnerabilities Equities Policy and Process for the United States Government." 15 Nov. 2017, www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF. Accessed 17 Oct. 2020.

67 US White House. "Vulnerabilities Equities Policy and Process for the United States Government." 15 Nov. 2017, p.6. www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF. Accessed 17 Oct. 2020.

68 This includes: the Office of Management and Budget; Office of the Director of National Intelligence (to include Intelligence Community-Security Coordination Center; Department of the Treasury; Department of State; Department of Justice (to include the Federal Bureau of Investigation and the National Cyber Investigative Joint Task Force); Department of Homeland Security (to include the National Cybersecurity Communications and Integration Center and the United States Secret Service); Department of Energy; Department of Defense (including the National Security Agency (including Information Assurance and Signals Intelligence elements)); United States Cyber Command, and DoD Cyber Crime Center; Department of Commerce; and the Central Intelligence Agency. US White House. "Vulnerabilities Equities Policy and Process for the United States Government." 15 Nov. 2017, p. 3 www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF. Accessed 17 Oct. 2020.

69 US White House. "Vulnerabilities Equities Policy and Process for the United States Government." 15 Nov. 2017, www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF. Accessed 17 Oct. 2020.

70 US White House. "Vulnerabilities Equities Policy and Process for the United States Government." 15 Nov. 2017, www.whitehouse.gov/sites/whitehouse.gov/files/images/External%20-%20Unclassified%20VEP%20Charter%20FINAL.PDF. Accessed 17 Oct. 2020.

71 Volz, Dustin. "White House Expands Use of Cyber Weapons but Stays Secretive on Policies" Wall Street Journal, 30 Dec. 2019, www.wsj.com/articles/white-house-expands-use-of-cyber-weapons-but-stays-secretive-on-policies-11577728030. Accessed 17 Oct. 2020.

72 The FBI is the only law enforcement member in the IC. Office of the Director of National Intelligence. "Members of the IC." DNI, www.dni.gov/index.php/what-we-do/members-of-the-ic. Accessed 17 Oct. 2020.

73 US Office of the Director of National Intelligence. "National Intelligence Strategy of the United States." 2019, p. 11. https://www.dni.gov/files/ODNI/documents/National_Intelligence_Strategy_2019.pdf. Accessed 20 Aug. 2020

74 US Department of Defense. "Summary: Department of Defense Cyber Strategy 2018." Sept. 2018. https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF. Accessed 18 Oct. 2020.

75 Whitley, Sean and Strom, Blake. "7 Steps for an APT Detection Playbook using ATT&CK™" 11 Aug 2017, https://www.mitre.org/capabilities/cybersecurity/overview/cybersecurity-blog/7-steps-for-an-apt-detection-playbook-using/. Accessed 17 Oct, 2020; Palo Alto Networks. "Unveiling 11 New Adversary Playbooks." 30 July 2019. https://unit42.paloaltonetworks.com/unveiling-11-new-adversary-playbooks/. Accessed 17 Oct. 2020

76 Office of the Inspector General of the Intelligence Community. "Unclassified Joint Report on the Implementation of the Cybersecurity Information Sharing Act of 2015." 19 Dec. 2019, p. 28. oig.justice.gov/reports/2019/AUD-2019-005-U.pdf#page=1. Accessed 17 Oct. 2020.

77 Johnson, Chris et al. "Guide to Cyber Threat Information Sharing." US National Institute of Standards and Technology, Oct. 2016 nvlpub,s.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-150.pdf. Accessed 17 Oct. 2020.

78 Examples include the FBI's Private Industry Notifications (PINS), the FBI Liaison Alert System (FLASH), and the FBI and DHS Joint Analysis Reports (JARs) and Joint Technical Advisories (JTAs). US Department of Justice. "Report of the Attorney General's Cyber Digital Task Force." 2 July 2018, p. 84. https://www.justice.gov/ag/page/file/1076696/download Accessed 4 Aug. 2020.

79 These agencies include CISA Watch, USSS Field Offices, Electronic Crimes Task Forces, ICE HSI Field Offices, ICE HSI Cyber Crimes Center, FBI Field Offices, Cyber Task Forces, and Law Enforcement Online Portal. US Department of Justice. "Law Enforcement Cyber Incident Reporting." www.justice.gov/usao-ct/page/file/906222/download. Accessed 17 Oct. 2020.

80 The ONCA could look at the feasibility of implementing the Cyberspace Solarium Commission's Joint Collaborative Environment and/or the President's National Infrastructure Advisory Council's Critical Infrastructure Command Center. US Cyberspace Solarium Commission. "CSC Final Report." March 2020, drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view. Accessed 17 Oct. 2020; President's National Infrastructure Advisory Council, "Transforming the U.S. Cyber Threat Partnership." Cybersecurity and Infrastructure Security Agency, 12 Dec. 2019, www.cisa.gov/sites/default/files/publications/NIAC-Transforming-US-Cyber-Threat-PartnershipReport-FINAL-508.pdf. Accessed 17 Oct. 2020.

81 US Federal Emergency Management Agency. "Critical Infrastructure: Long-term Trends and Drivers and Their Implications for Emergency Management." June 2011, p. 2. https://www.fema.gov/pdf/about/programs/oppa/ critical_infrastructure_paper.pdf. Accessed 17 Oct. 2020.

82 United States, Congress, Senate Select Committee on Intelligence. "Russian Active Measures Campaigns and Interference in the 2016 U.S. Election: Volume 5: Counterintelligence Threats and Vulnerabilities." 116th Congress, 1st Session, p. 199. https://www.intelligence.senate.gov/sites/default/files/documents/report_volume5.pdf. Accessed 20 Oct. 2020.

83 UN Security Council, "Report of a Panel of Experts established pursuant to resolution 1874 (2009)." 2 March 2020, p. 65. undocs.org/S/2020/151. Accessed 17 Oct. 2020.

84 Congress could also consider introducing and passing legislation requiring the ODNI to perform this NIE.

85 US White House. "National Cyber Strategy of the United States of America." Sept. 2018, p. 10-11, https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf. Accessed 17 Oct. 2020; US Government Accountability Office. "Cybersecurity: Clarity of Leadership Urgently Needed to Fully Implement the National Strategy." Sept. 2020. www.gao.gov/assets/710/709555.pdf?utm_campaign=wp_the_cybersecurity_202&utm_medium=email&utm_source=newsletter&wpisrc=nl_cybersecurity202. Accessed 17 Oct. 2020.

86 Gaskew, Brandon. "Reader's Guide to Understanding the US Cyber Enforcement Architecture and Budget." Third Way, 21 Feb. 2019, www.thirdway.org/memo/readers-guide-to-understanding-the-us-cyber-enforcement-architecture-and-budget. Accessed 17 Oct. 2020.

87 Examples include National Cyber Incident Response Plan, DOJ's Cyber Digital Task Force Report, PPD-41, and DOJ's reporting framework. US Department of Homeland Security. "National Cyber Incident Response Plan." Dec 2016, https://us-cert.cisa.gov/sites/default/files/ncirp/National_Cyber_Incident_Response_Plan.pdf Accessed 17 Oct. 2020; US Department of Justice. "Report of the Attorney General's Cyber Digital Task Force." 2 July 2018, p. 95. www.justice.gov/ag/page/file/1076696/download. Accessed 17 Oct. 2020; White House. "Presidential Policy Directive—United States Cyber Incident Coordination." White House Obama Archives, 26 July 2016, obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident. Accessed 17 Oct. 2020; United States, Congress, House. United States Code. Title 18. Legal Information Institute, Cornell Law School, law.cornell.edu/uscode/text/18. Accessed 17 Oct. 2020; US Department of Justice, CCIPS. "Reporting Computer, Internet-related, Or Intellectual Property Crime." 18 Dec. 2018, justice.gov/

criminal-ccips/reporting-computer-internet-related-or-intellectual-property-crime. Accessed 17 Oct. 2020.

88 "Department of Justice Announces Disruption of Hundreds of Online COVID-19 Related Scams." Press Release, US Department of Justice, 22 Apr. 2020, www.justice.gov/opa/pr/department-justice-announces-disruption-hundreds-online-covid-19-related-scams. Accessed 17 Oct. 2020.

89 Recommended proposals to improve federal and SLTT coordination should account for the assessment performed under Recommendation 11.3.

90 See, for example, the United States Secret Service Mission Improvement and Realignment Act of 2020 (S. 3636). United States, Congress, Senate. S. 3636. Introduced 6 May 2020, www.congress.gov/bill/116th-congress/senate-bill/3636?s=1&r=11. Accessed 17 Oct. 2020.

91 Brunner, Maggie. "Challenges and Opportunities in State and Local Cybercrime Enforcement." Journal of National Security Law & Policy, Vol. 10:563, May 2020, jnslp.com/wp-content/uploads/2020/05/Challenges-and-Opportunities-in-State-and-Local-Cybercrime-Enforcement.pdf. Accessed 17 Oct. 2020.

92 Finklea, Kristin and Theohary, Catherine A. "Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement." Congressional Research Service, 15 Jan. 2015, fas.org/sgp/crs/misc/R42547.pdf. Accessed 17 Oct. 2020.

93 Due to a lack of a uniformed definition of cybercrime, it is unclear if federal law enforcement uses this definition of cyberspace. Finklea, Kristin and Theohary, Catherine A. "Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement." Congressional Research Service, 15 Jan. 2015, fas.org/sgp/crs/misc/R42547.pdf. Accessed 17 Oct. 2020.

94 Finklea, Kristin and Theohary, Catherine A. "Cybercrime: Conceptual Issues for Congress and U.S. Law Enforcement." Congressional Research Service, 15 Jan. 2015, fas.org/sgp/crs/misc/R42547.pdf. Accessed 17 Oct. 2020.

95 Hindocha, Anisha. "2020 Reader's Guide to Understanding the US Cyber Enforcement Architecture and Budget." Third Way, 26 March 2020. https://www.thirdway.org/report/2020-readers-guide-to-understanding-the-us-cyber-enforcement-architecture-and-budget. Accessed 17 Oct 2020.

96 Garcia, Michael and Hindocha, Anisha. "Where Are We Now? Examining the Trump Administration's Efforts to Combat Cybercrime." Third Way, 22 June 2020, www.thirdway.org/report/where-are-we-now-examining-the-trump-administrations-efforts-to-combat-cybercrime. Accessed 17 Oct. 2020.

97 For example, the National Computer Forensic Institute (NCFI) and the National Domestic Communications Assistance Center (NDCAC). US Secret Service. "The National Computer Forensics Institute." https://www.ncfi.usss.gov/ncfi/index.xhtml;jsessionid=cIlu92GbActa4w8fSCjlTKls?dswid=6476. Accessed 17 Oct. 2020. The Federal Bureau of Investigation. "National Domestic Communications Assistance Center." https://ndcac.fbi.gov/ Accessed 17 Oct. 2020.

98 NW3C trained over 100,000 law enforcement and criminal justice personnel between October 2019 to September 2020. National White-Collar Crime Center. Interview by Michael Garcia, September 2020.

99 The US Cyberspace Solarium Commission made a similar recommendation in their first white paper, "Cybersecurity Lessons Learned from the Pandemic." United States of America Cyberspace Solarium Commission, May 2020, drive.google.com/file/d/1wCHVtIFlw84uZIPOTZe2nkdGau15fLAQ/view. Accessed 17 Oct. 2020.

100 US Department of Justice, CCIPS. "Cybercrime Symposium." www.justice.gov/criminal-ccips/cybercrime-symposium. Accessed 17 Oct. 2020.

101 Lyngas, Sean. "Inside the FBI's quiet 'ransomware summit'." CyberScoop, 6 Nov. 2019, www.cyberscoop.com/fbi-ransomware-summit/. Accessed 17 Oct. 2020; "HSI New York hosts 1st annual Cyber Crime Symposium." Press Release, United States Department of Homeland Security, Immigration and Customs Enforcement, 19 Apr. 2019, www.ice.gov/news/releases/hsi-new-york-hosts-1st-annual-cyber-crime-symposium. Accessed 17 Oct. 2020; "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, www.secretservice.gov/data/press/releases/2019/19-MAY/19_0521_USSS_dhs-atlanta-cyber-incident-response.pdf. Accessed 17 Oct. 2020.

102 Other events include the Ransomware Campaign workshops, Business Email Compromise Campaign, and the FBI's General Counsel Cyber Summits. US Department of Justice. "Report of the Attorney General's Cyber Digital Task Force." 2 July 2018, p. 84. www.justice.gov/ag/page/file/1076696/download. Accessed 17 Oct. 2020.

103 For example, the National Governors Association, the US Conference of Mayors, the International Association of Chiefs of Police, and others.

104 For example, Blackhat, RSA, RightsCon, DEFCON, South by Southwest (SXSW), and others.

105 Garcia, Michael and Hindocha, Anisha. "Where Are We Now? Examining the Trump Administration's Efforts to Combat Cybercrime." Third Way, 22 June 2020, www.thirdway.org/report/where-are-we-now-examining-the-trump-administrations-efforts-to-combat-cybercrime. Accessed 17 Oct. 2020.

106 US Government Accountability Office. "Cybersecurity: Clarity of Leadership Urgently Needed to Fully Implement the National Strategy." Sept. 2020, p. 31. www.gao.gov/assets/710/709555.pdf?utm_campaign=wp_the_cybersecurity_202&utm_medium=email&utm_source=newsletter&wpisrc=nl_cybersecurity202. Accessed 17 Oct. 2020.

107 US Department of Homeland Security. "FY 2019-2021 Annual Performance Report." www.dhs.gov/sites/default/files/publications/dhs_fy_2019-2021_apr_final.pdf. Accessed 17 Oct. 2020; US Department of Justice. "Combat Cyber-Enabled Threats and Attacks." www.performance.gov/justice/FY2020_july_Combat_Cyber-Enabled_Threats_and_Attacks.pdf. Accessed 17 Oct. 2020.

108 Mehta, Ishan. "The Need for Better Metrics on Cybercrime." Third Way, 1 Oct 2019, https://www.thirdway.org/memo/the-need-for-better-metrics-on-cybercrime. Accessed 17 Oct. 2020.

109 In their FY 2019 Congressional Justification, the US Secret Service included the number of law enforcement officials trained in cybercrime and forensics and how much financial loss they want to prevent. US Department of Homeland Security, Secret Service. "Budget Overview: Fiscal Year 2019 Congressional Justification." www.dhs.gov/sites/default/files/publications/U.S.%20Secret%20Service.pdf. Accessed 17 Oct. 2020.

110 This should include analyzing what performance targets could be established for different enforcement agencies, being careful to not set skewed incentives that reward reaching these targets at the expense of pursuing more complicated and time-consuming cases. Mehta, Ishan. "The Need for Better Metrics on Cybercrime." Third Way, 1 Oct. 2019, www.thirdway.org/memo/the-need-for-better-metrics-on-cybercrime. Accessed 17 Oct. 2020.

111 Mehta, Ishan. "The Need for Better Metrics on Cybercrime." Third Way, 1 Oct. 2019, www.thirdway.org/memo/the-need-for-better-metrics-on-cybercrime. Accessed 17 Oct. 2020.

112 US Federal Bureau of Investigation, Criminal Justice Information Services. "National Incident-Based Reporting System." www.fbi.gov/services/cjis/ucr/nibrs. Accessed 17 Oct. 2020.

113 National Academy of Sciences, Engineering, and Medicine. "Modernizing Crime Statistics: Report 2: New Systems for Measuring Crime." The National Academies Press, 2018, www.nap.edu/read/25035/chapter/10#127 Accessed 17 Oct. 2020.

114 US Federal Bureau of Investigation. "Crime Data Explorer." https://crime-data-explorer.fr.cloud.gov/. Accessed 17 Oct 2020.

115 The CJIS Advisory Policy Board is responsible for reviewing appropriate policy, technical, and operational issues related to CJIS Division programs. US Federal Bureau of Investigation, Criminal Justice Information Services. "The CJIS Advisory Process: A Shared Management Concept." www.fbi.gov/services/cjis/the-cjis-advisory-process. Accessed 17 Oct. 2020.

116 National Academies of Sciences, Engineering, and Medicine. "Modernizing Crime Statistics: Report 1: Defining and Classifying Crime." The National Academies Press, 2016, www.nap.edu/catalog/23492/

modernizing-crime-statistics-report-1-defining-and-classifying-crime. Accessed 17 Oct. 2020; National Academy of Sciences, Engineering, and Medicine. "Modernizing Crime Statistics: Report 2: New Systems for Measuring Crime." The National Academies Press, 2018, www.nap.edu/catalog/25035/modernizing-crime-statistics-report-2-new-systems-for-measuring-crime. Accessed 17 Oct. 2020 .

117 National Academies of Sciences, Engineering, and Medicine. "Modernizing Crime Statistics: Report 1: Defining and Classifying Crime." The National Academies Press, 2016, www.nap.edu/catalog/23492/modernizing-crime-statistics-report-1-defining-and-classifying-crime. Accessed 17 Oct. 2020.

118 These crimes included (1) Damage to computer systems (to include Distributed Denial of Service (DDoS) attacks, ransomware attacks, and destructive attacks); (2) Data theft (to include hacks aimed at stealing personal identifiable information and the theft of intellectual property); (3) Fraud/carding schemes; (4) Crimes threatening personal privacy (to include sextortion, non-consensual pornography (frequently called revenge pornography), cyber-enabled stalking and harassment, swatting, and doxxing); and (5) Crimes threatening critical infrastructure. US Department of Justice. "Report of the Attorney General's Cyber Digital Task Force." 2 July 2018, www.justice.gov/ag/page/file/1076696/download. Accessed 18 Oct. 2020.

119 US Department of Justice, Bureau of Justice Assistance. "Paul Coverdell Forensic Science Improvement Grants Program – Competitive, FY 2020 Competitive Grant Solicitation." 20 Apr. 2020, bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/bja-2020-18433.pdf. Accessed 18 Oct. 2020; US Department of Justice, Bureau of Justice Assistance. "2020 State Justice Statistics Program for Statistical Analysis Centers, FY 2020 Grant Solicitation." 12 Feb. 2020, www.bjs.gov/content/pub/pdf/sjssac20_sol.pdf. Accessed 18 Oct. 2020.

120 Three percent of the JAG grant is set aside to assist with the transition to NIBRS. US Department of Justice, Bureau of Justice Assistance. "Edward Byrne Memorial Justice Assistance Grant (JAG) Program." 2020, bja.ojp.gov/program/jag/overview. Accessed 18 Oct. 2020.

121 34 USC 41305. "Hate crime statistics." United States Code, US Government Publishing Office, 28 Oct. 2009, uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title34-section41305&num=0&edition=prelim. Accessed 18 Oct. 2020.

122 22 USC Ch. 78. "Trafficking Victims Protection." United States Code, 28 Oct. 2000, https://www.law.cornell.edu/uscode/text/22/chapter-78. Accessed 18 Oct 2020.

123 Although federal law enforcement agencies are required to report crime and arrest data through the FBI by the Uniform Federal Crime Reporting Act (P.L. 100-690), many do not do so. Mehta, Ishan. "The Need for Better Metrics on Cybercrime." Third Way, 1 Oct. 2019, www.thirdway.org/memo/the-need-for-better-metrics-on-cybercrime. Accessed 18 Oct. 2020.

124 Mehta, Ishan. "The Need for Better Metrics on Cybercrime." Third Way, 1 Oct. 2019, www.thirdway.org/memo/the-need-for-better-metrics-on-cybercrime. Accessed 18 Oct. 2020.

125 Mehta, Ishan. "The Need for Better Metrics on Cybercrime." Third Way, 1 Oct. 2019, www.thirdway.org/memo/the-need-for-better-metrics-on-cybercrime. Accessed 18 Oct. 2020.

126 Decker, Eileen. "Full Count?: Crime Rate Swings, Cybercrime Misses and Why We Don't Really Know the Score." Journal of National Security Law & Policy, Vol. 10:583, May 2020, jnslp.com/wp-content/uploads/2020/05/Crime-Rate-Swings-Cybercrime-Misses.pdf. Accessed 18 Oct. 2020.

127 "Crimes Americans worry about most in 2019." Statista Research Department, 11 Dec. 2019, www.statista.com/statistics/339735/crime-worries-in-the-united-states/. Accessed 18 Oct. 2020; Eoyang, Mieke, et al. "To Catch a Hacker: Toward a comprehensive strategy to identify, pursue, and punish malicious cyber actors." Third Way, 29 Oct. 2018, www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors. Accessed 18 Oct. 2020.

128 Reinhart, RJ. "One in Four Americans Have Experienced Cybercrime." Gallup, 11 Dec. 2018, news.gallup.com/poll/245336/one-four-americans-experienced-cybercrime.aspx. Accessed 18 Oct. 2020.

129 Center for Victim Research. "Research Brief: Identity Theft and Fraud." ncvc.dspacedirect.org/bitstream/item/1228/CVR%20Research%20Syntheses_Identity%20Theft%20and%20Fraud_Brief.pdf. Accessed 18 Oct. 2020.

130 US Department of Justice. "Report of the Attorney General's Cyber Digital Task Force." 2 July 2018, www.justice.gov/ag/page/file/1076696/download. Accessed 18 Oct. 2020.

131 US Department of Justice, Office for Victims of Crime. "Attorney General Guidelines for Victim and Witness Assistance." May 2012, www.justice.gov/sites/default/files/olp/docs/ag_guidelines2012.pdf. Accessed 18 Oct. 2020; US Department of Justice, Office of the Inspector General. "Audit of the Federal Bureau of Investigation's Cyber Victim Notification Process." March 2019, oig.justice.gov/reports/2019/a1923.pdf#page=1. Accessed 18 Oct. 2020.

132 42 U.S.C. § 10607 and 18 U.S.C. § 3771. For more information regarding these statutes, please see US Department of Justice. "Report of the Attorney General's Cyber Digital Task Force." 2 July 2018, p. 112. www.justice.gov/ag/page/file/1076696/download. Accessed 18 Oct. 2020.

133 An OVC commissioned report found that "few services and resources exist to address the specific trauma-needs of these victims." Center for Victim Research. "Research Brief: Identity Theft and Fraud." ncvc.dspacedirect.org/bitstream/item/1228/CVR%20Research%20Syntheses_Identity%20Theft%20and%20Fraud_Brief.pdf. Accessed 18 Oct. 2020. See also US Federal Register. "Victims of Crime Act Victim Assistance Program." 8 Jul. 2016, www.federalregister.gov/documents/2016/07/08/2016-16085/victims-of-crime-act-victim-assistance-program. Accessed 18 Oct. 2020.

134 The nonprofit Cybercrime Support Network received a $1 million cooperative agreement from DHS to develop a "Reporting and Threat information Sharing Pilot" program to standardize reporting structure for state and local law enforcement. "Cybercrime Support Network Awarded $1 Million Cooperative Agreement from the U.S. Department of Homeland Security to Create a Uniform Cybercrime Reporting Structure." Press Release. Cybercrime Support Network, 21 Nov. 2019, www.globenewswire.com/news-release/2019/11/21/1950799/0/en/Cybercrime-Support-Network-Awarded-1-Million-Cooperative-Agreement-from-the-U-S-Department-of-Homeland-Security-to-Create-a-Uniform-Cybercrime-Reporting-Structure.html. Accessed 18 Oct. 2020. This assessment should also study countries that have established similar call centers for cybercrime victims, such as Australia, and determine the cost of implementing the Cyberspace Solarium Commission's recommendation on providing grants to nonprofits that assist in victim support efforts.

135 US Department of Justice, Office of the Inspector General. "Audit of the Federal Bureau of Investigation's Cyber Victim Notification Process." March 2019, oig.justice.gov/reports/2019/a1923.pdf#page=1. Accessed 18 Oct. 2020.

136 The Cybercrime Working Group should also consider whether to expand this to local law enforcement agencies, insurance companies, and other public and not-for-profit organizations to retrieve anonymous, aggregated data that they collect on cybercrime occurrences. US Department of Justice, Bureau of Justice Statistics. "Data Collection: National Computer Security Survey." 2006, www.bjs.gov/index.cfm?ty=dcdetail&iid=260. Accessed 18 Oct. 2020.

137 Mehta, Ishan. "The Need for Better Metrics on Cybercrime." Third Way, 1 Oct. 2019, www.thirdway.org/memo/the-need-for-better-metrics-on-cybercrime. Accessed 18 Oct. 2020.

138 US Department of Justice, Computer Crime and Intellectual Property Section Criminal Division. "Best Practices for Victim Response and Reporting of Cyber Incidents." Apr. 2015, www.justice.gov/sites/default/files/opa/speeches/attachments/2015/04/29/criminal_division_guidance_on_best_practices_for_victim_response_and_reporting_cyber_incidents2.pdf. Accessed 18 Oct. 2020.

139 Center for Victim Research. "Research Brief: Identity Theft and Fraud." ncvc.dspacedirect.org/bitstream/item/1228/CVR%20Research%20Syntheses_Identity%20Theft%20and%20Fraud_Brief.pdf. Accessed 18 Oct. 2020.

140 US Federal Bureau of Investigation, Criminal Justice Information Services. "Law Enforcement Enterprise Portal." www.fbi.gov/services/cjis/leep. Accessed 18 Oct. 2020; US Federal Bureau of

Investigation. "eGuardian." www.fbi.gov/resources/law-enforcement/eguardian. Accessed 18 Oct. 2020; US Federal Bureau of Investigation, Criminal Justice Information Services. "National Data Exchange (N-DEx) System." www.fbi.gov/services/cjis/ndex. Accessed 18 Oct. 2020.

141 US Federal Trade Commission. "Consumer Sentinel Network." www.ftc.gov/system/files/attachments/consumer-sentinel-network/191001_sentinel_onepager_v5.pdf. Accessed 18 Oct. 2020.

142 Garcia, Michael. "Meet the Threat: Memo on State Cybersecurity Centers." National Governors Association, www.nga.org/wp-content/uploads/2019/09/Memo-on-State-Cybersecurity-Centers-v5.pdf. Accessed 18 Oct. 2020.

143 US Department of Justice, Bureau of Justice Assistance. "2020 State Justice Statistics Program for Statistical Analysis Centers, FY 2020 Grant Solicitation." 12 Feb. 2020, www.bjs.gov/content/pub/pdf/sjssac20_sol.pdf. Accessed 18 Oct. 2020.

144 For example, New Jersey, California, and New Hampshire.

145 Garcia, Michael. "Memo on State Cybersecurity Centers." National Governors Association, www.nga.org/wp-content/uploads/2019/09/Memo-on-State-Cybersecurity-Centers-v5.pdf. Accessed 18 Oct. 2020.

146 US Department of Justice, Bureau of Justice Assistance. "2020 State Justice Statistics Program for Statistical Analysis Centers, FY 2020 Grant Solicitation." 12 Feb. 2020, www.bjs.gov/content/pub/pdf/sjssac20_sol.pdf. Accessed 18 Oct. 2020; U.S. Department of Justice, Bureau of Justice Statistics. "State Justice Statistics Program for Statistical Analysis Centers, 2009." www.bjs.gov/content/pub/pdf/sjssac09sol.pdf. Accessed 18 Oct. 2020.

147 "Cybersecurity Supply/Demand Heat Map." CyberSeek, www.cyberseek.org/heatmap.html. Accessed 18 Oct. 2020.

148 US Department of Commerce and US Department of Homeland Security. "A Report to the President On Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future." 30 May 2018, www.nist.gov/system/files/documents/2018/07/24/eo_wf_report_to_potus.pdf. Accessed 18 Oct. 2020.

149 US White House. "Executive Order on America's Cybersecurity Workforce." Executive Order, 2 May 2019, www.whitehouse.gov/presidential-actions/executive-order-americas-cybersecurity-workforce/. Accessed 18 Oct. 2020; US Department of Commerce and US Department of Homeland Security. "A Report to the President On Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future." 30 May 2018, www.nist.gov/system/files/documents/2018/07/24/eo_wf_report_to_potus.pdf. Accessed 18 Oct. 2020.

150 In July 2016, OMB and OPM issued a memo to all federal agencies to overcome cybersecurity workforce challenges, entitled "2016 Federal Cybersecurity Workforce Strategy." Executive Office of the President, Office of Management and Budget. "Federal Cybersecurity Workforce Strategy." 12 July 2016, chcoc.gov/content/federal-cybersecurity-workforce-strategy. Accessed 18 Oct. 2020.

151 US Department of Commerce and US Department of Homeland Security. "A Report to the President On Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future." 30 May 2018, www.nist.gov/system/files/documents/2018/07/24/eo_wf_report_to_potus.pdf. Accessed 18 Oct. 2020; US Cyberspace Solarium Commission. "United States of America Cyberspace Solarium Commission Report." March 2020, drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view. Accessed 18 Oct. 2020.

152 US Department of Justice, Bureau of Justice Assistance. "BJA FY 19 Student Computer and Digital Forensics Educational Opportunities Program." 25 Apr. 2019, bja.ojp.gov/funding/opportunities/bja-2019-16290. Accessed 18 Oct. 2020.

153 The proposed Cyber Security Exchange Act (S.429) would perform similar initiatives and could be used as a model. United States, Congress, Senate, Cyber Security Exchange Act. Congress.gov, www.congress.gov/bill/116th-congress/senate-bill/429/text?q=%7B%22search%22%3A%5B%22klobuchar%22%5D%7D&r=64&s=2. 116th Congress, 1st session, S. 429. Accessed 18 Oct. 2020; Executive Office

of the President, Office of Management and Budget. "Federal Cybersecurity Workforce Strategy." 12 July 2016, chcoc.gov/content/federal-cybersecurity-workforce-strategy. Accessed 18 Oct. 2020; President Donald Trump White House. "Executive Order on America's Cybersecurity Workforce." Executive Order, 2 May 2019, www.whitehouse.gov/presidential-actions/executive-order-americas-cybersecurity-workforce/. Accessed 18 Oct. 2020; US Cyberspace Solarium Commission. "United States of America Cyberspace Solarium Commission Report." March 2020, drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view. Accessed 18 Oct. 2020.

154 PL 114-113. For more information, please see US Department of Commerce, National Institute of Standards and Technology. "Federal Cybersecurity Coding Structure." 18 Oct. 2017, www.nist.gov/file/394236. Accessed 18 Oct. 2020.

155 US Cyberspace Solarium Commission. "Growing a Stronger Federal Cyber Workforce." CSC White Paper #3, Sept. 2020, drive.google.com/file/d/1WGNHpVmf4X12zv6DWuq9V4GtKF3jz92e/view. Accessed 18 Oct. 2020; US Department of Justice. "Report of the Attorney General's Cyber Digital Task Force." 2 July 2018, p. 98. www.justice.gov/ag/page/file/1076696/download. Accessed 18 Oct. 2020.

156 US Department of Commerce and US Department of Homeland Security. "A Report to the President On Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future." 30 May 2018, www.nist.gov/system/files/documents/2018/07/24/eo_wf_report_to_potus.pdf. Accessed 18 Oct. 2020.

157 OPM estimates that minorities comprise 32% of the cyber workforce in the federal government. Executive Office of the President, Office of Management and Budget. "Federal Cybersecurity Workforce Strategy." 12 July 2016, chcoc.gov/content/federal-cybersecurity-workforce-strategy Accessed 18 Oct. 2020; US Department of Commerce and US Department of Homeland Security. "A Report to the President On Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future." 30 May 2018, www.nist.gov/system/files/documents/2018/07/24/eo_wf_report_to_potus.pdf. Accessed 18 Oct. 2020; US Cyberspace Solarium Commission. "United States of America Cyberspace Solarium Commission Report." March 2020, drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view. Accessed 18 Oct. 2020.

158 "Cybersecurity Career Pathway." CyberSeek, www.cyberseek.org/pathway.html. Accessed 18 Oct. 2020.

159 Gardiner, Christine. "How Educated Should Police Be?" National Police Foundation, www.policefoundation.org/study-examines-higher-education-in-policing/#:~:text=About%20one%20third%20(30.2%20percent,percent%20have%20a%20graduate%20degree. Accessed 18 Oct. 2020.

160 Garcia, Michael and Hindocha, Anisha. "Where Are We Now? Examining the Trump Administration's Efforts to Combat Cybercrime." Third Way, 22 June 2020, www.thirdway.org/report/where-are-we-now-examining-the-trump-administrations-efforts-to-combat-cybercrime. Accessed 18 Oct. 2020.

161 US Department of Commerce and US Department of Homeland Security. "A Report to the President On Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future." 30 May 2018, www.nist.gov/system/files/documents/2018/07/24/eo_wf_report_to_potus.pdf. Accessed 18 Oct. 2020; US Cyberspace Solarium Commission. "Growing a Stronger Federal Cyber Workforce." CSC White Paper #3, Sept. 2020, drive.google.com/file/d/1WGNHpVmf4X12zv6DWuq9V4GtKF3jz92e/view. Accessed 18 Oct. 2020.

162 Personnel should include police officers, investigators, prosecutors, clerks, judges, and public defenders. In 2019, BJS issued separate surveys to public defenders and prosecutors, with cybercrime a focus of area for the prosecutors' survey. US Department of Justice, Bureau of Justice Statistics. "National Survey of Prosecutors, 2019 (NSP19) Grant Solicitation." 24 May 2018, www.bjs.gov/content/pub/pdf/nsp19_sol.pdf. Accessed 18 Oct. 2020; US Department of Justice, Bureau of Justice Statistics. "Survey of Public Defenders (SPD) Grant Solicitation." 28 May 2019, www.bjs.gov/content/pub/pdf/spd_sol.pdf. Accessed 18 Oct. 2020.

163 US Department of Justice, Bureau of Justice Statistics. "National Survey of Prosecutors, 2019 (NSP19) Grant Solicitation." 24 May 2018, www.bjs.gov/content/pub/pdf/nsp19_sol.pdf. Accessed 18 Oct. 2020.

164 US Department of Commerce and US Department of Homeland Security. "A Report to the President On Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future." 30 May 2018, www.nist.gov/system/files/documents/2018/07/24/eo_wf_report_to_potus.pdf. Accessed 18 Oct. 2020.

165 US National Security Agency, Central Security Service. "National Centers of Academic Excellence in Cybersecurity." www.nsa.gov/resources/students-educators/centers-academic-excellence/. Accessed 18 Oct. 2020; Executive Office of the President, Office of Management and Budget. "Federal Cybersecurity Workforce Strategy." 12 July 2016, Chief Human Capital Officers Council, chcoc.gov/content/federal-cybersecurity-workforce-strategy. Accessed 18 Oct. 2020.

166 US Department of Justice. "Report of the Attorney General's Cyber Digital Task Force." 2 July 2018, p.98. www.justice.gov/ag/page/file/1076696/download. Accessed 18 Oct. 2020; US Department of Homeland Security, Office of the Secret Service. "James J. Rowley Training Center." www.secretservice.gov/join/training/training_rowley/. Accessed 18 Oct. 2020.

167 National Institute of Standards and Technology. "Cyber Range." 2018. https://www.nist.gov/system/files/documents/2018/02/13/cyber_ranges.pdf. Accessed 18 Oct 2020.

168 US Department of Justice. "Report of the Attorney General's Cyber Digital Task Force." 2 July 2018, www.justice.gov/ag/page/file/1076696/download. Accessed 18 Oct. 2020.

169 The Workforce Training Initiative trains employees on how to respond, investigate, and analyze cyber-related cross-programmatic matters. The On the Job Training Initiative places participants on a cyber squad for six months to become experienced in handling cybercrime cases prior to returning to their previous squad. US Department of Justice. "Report of the Attorney General's Cyber Digital Task Force." 2 July 2018, p. 98. www.justice.gov/ag/page/file/1076696/download. Accessed 15 Oct. 2020.

170 CIO Council. "Federal Cyber Reskilling Academy." www.cio.gov/programs-and-events/reskilling/. Accessed 18 Oct. 2020.

171 These categories include cybercrime investigator, law enforcement forensics analysts, and cyber defense forensics analysts. US Cyberspace Solarium Commission. "Growing a Stronger Federal Cyber Workforce." CSC White Paper #3, Sept. 2020, drive.google.com/file/d/1WGNHpVmf4X12zv6DWuq9V4GtKF3jz92e/view. Accessed 17 Oct. 2020.

172 United States, Congress. United States Code. Title 37, Chapter 5, Special and Incentive Pays. Legal Information Institute, Cornell Law School, www.law.cornell.edu/uscode/text/37/chapter-5. Accessed 18 Oct. 2020.

173 Carter, William, et al. "Low-Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge" Center for Strategic and International Studies, 2018 July, p.12. csis-website-prod.s3.amazonaws.com/s3fs-public/publication/180725_Carter_DigitalEvidence.pdf?tAGR_DvxRdp0RspiGYNGcGKTUjrGY3rN. Accessed 18 Oct. 2020.

174 Carter, William, et al. "Low-Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge" Center for Strategic and International Studies, 2018 July, p.12. csis-website-prod.s3.amazonaws.com/s3fs-public/publication/180725_Carter_DigitalEvidence.pdf?tAGR_DvxRdp0RspiGYNGcGKTUjrGY3rN. Accessed 18 Oct. 2020.

175 Carter, William, et al. "Low-Hanging Fruit: Evidence-Based Solutions to the Digital Evidence Challenge" Center for Strategic and International Studies, 2018 July, csis-website-prod.s3.amazonaws.com/s3fs-public/publication/180725_Carter_DigitalEvidence.pdf?tAGR_DvxRdp0RspiGYNGcGKTUjrGY3rN. Accessed 18 Oct. 2020.

176 United States, Congress, House. Technology in Criminal Justice Act of 2019. Congress.gov, www.congress.gov/bill/116th-congress/house-bill/5227/text. 116th Congress, 1st session, H.R. 5227. Accessed 18 Oct. 2020.

177 United States, Congress. United States Code. Title 6, Chapter 1, Section 383, National Computer Forensics Institute. House.gov, uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title6-section383&num=0&edition=prelim. Accessed 18 Oct. 2020.

178 Goodison, Sean, et al. "Digital Evidence and the US Criminal Justice System: Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence." Priority Criminal Justice Needs Initiative, 2015. https://www.ncjrs.gov/pdffiles1/nij/grants/248770.pdf. Accessed 18 Oct. 2020.

179 "Digital Evidence Task Force: Executive Primer." The International Association of Chiefs of Police, 2019, www.theiacp.org/sites/default/files/2019-11/IACP_Digital_Evidence_Task_Force.pdf. Accessed 18 Oct. 2020.

180 "Regional Computer Forensics Laboratory." Homepage, www.rcfl.gov/. Accessed 18 Oct. 2020.

181 US Department of Justice, Bureau of Justice Assistance. "Paul Coverdell Forensic Science Improvement Grants Program." bja.ojp.gov/program/coverdell/overview. Accessed 18 Oct. 2020.

182 This was the last time this survey was conducted and the last comprehensive survey administered that assessed state and local cybercrime enforcement capabilities.

183 "The Role of Local Law Enforcement Agencies in Preventing and Investigating Cybercrime" Police Executive Research Forum, Apr. 2014, p. 7. policeforum.org/assets/docs/Critical_Issues_Series_2/the%20role%20of%20local%20law%20enforcement%20agencies%20in%20preventing%20and%20investigating%20cybercrime%202014.pdf. Accessed 18 Oct. 2020.

184 DOJ could look to the Homeland Security Grant Program as a potential model, which uses a survey to assess a state's cybersecurity readiness as a precondition to using the grant for cyber needs. Center for Internet Security. "Nationwide Cybersecurity Review (NCSR)." www.cisecurity.org/ms-isac/services/ncsr/. Accessed 18 Oct. 2020.

185 This includes grants within the Homeland Security Grant Program. Federal Emergency Management Agency. "Homeland Security Grant Program." 2020. https://www.fema.gov/grants/preparedness/homeland-security. Accessed 17 Oct. 2020.

186 These areas include law enforcement programs; prosecution and court programs; prevention and education programs; corrections and community corrections programs; drug treatment and enforcement programs; planning, evaluation, and technology improvement programs; crime victim and witness programs (other than compensation); and mental health programs and related law enforcement and corrections programs, including behavioral programs and crisis intervention teams. US Department of Justice, Bureau of Justice Assistance. "FY 2020 Edward Byrne Memorial Justice Assistance Grant (JAG) Program Local Formula Solicitation." 9 July 2020, bja.ojp.gov/funding/opportunities/bja-2020-17276. Accessed 18 Oct. 2020.

187 US Department of Justice, Bureau of Justice Assistance. "FY 2020 Edward Byrne Memorial Justice Assistance Grant (JAG) Program Local Formula Solicitation." 9 July 2020, bja.ojp.gov/funding/opportunities/bja-2020-17276. Accessed 18 Oct. 2020.

188 US Department of Justice, Bureau of Justice Assistance. "Edward Byrne Justice Assistance Grant (JAG) Program Fact Sheet." 18 May 2020, bja.ojp.gov/sites/g/files/xyckuh186/files/media/document/jag-fact-sheet-5-2020.pdf. Accessed 18 Oct. 2020.

189 "Crime worries in the United States 2019." Statista Research Department. 11 Dec 2019, www.statista.com/statistics/339735/crime-worries-in-the-united-states/. Accessed 18 Oct. 2020.

190 United States, Congress. United States Code. Title 34, Section 10157, Reserved Funds. Legal Information Institute, Cornell Law School, www.law.cornell.edu/uscode/text/34/10157. Accessed 18 Oct. 2020.

191 US Department of Justice, Bureau of Justice Assistance. "FY 2020 Edward Byrne Memorial Justice Assistance Grant (JAG) Program Local Formula Solicitation." 9 July 2020, bja.ojp.gov/funding/opportunities/bja-2020-17276. Accessed 18 Oct. 2020.

192 United States, Congress. United States Code. Title 34, Section 10156, Formula. Legal Information Institute, Cornell Law School, https://www.law.cornell.edu/uscode/text/34/10156. Accessed 18 Oct. 2020.

193 US Department of Justice, Office of Community Oriented Policing Services. "About the COPS Office." cops.usdoj.gov/aboutcops. Accessed 18 Oct. 2020.

194 Brunner, Maggie. "Challenges and Opportunities in State and Local Cybercrime Enforcement." Journal of National Security Law & Policy, Vol. 10:563, May 2020, jnslp.com/wp-content/uploads/2020/05/Challenges-and-Opportunities-in-State-and-Local-Cybercrime-Enforcement.pdf. Accessed 18 Oct. 2020.

195 US Department of Justice, Office of the Inspector General. "Audit of the Federal Bureau of Investigation's Implementation of Its Next Generation Cyber Initiative." Jul 2015, p. 19. oig.justice.gov/reports/2015/a1529.pdf. Accessed 18 Oct. 2020.

196 Task forces in each of the 56 field offices that synchronize domestic cyber threat investigations in the local community through information sharing, incident response, and joint enforcement and intelligence actions. As of 2015, Cyber Task Forces caseloads were 54% criminal related matters and 46% national-security matters. US Department of Justice, Federal Bureau of Investigation. "Cyber Task Forces: Building Alliances to Improve the Nation's Cybersecurity." www.fbi.gov/file-repository/cyber-task-forces-fact-sheet.pdf/view. Accessed 18 Oct. 2020; US Department of Justice, Office of the Inspector General. "Audit of the Federal Bureau of Investigation's Implementation of Its Next Generation Cyber Initiative." Jul 2015, oig.justice.gov/reports/2015/a1529.pdf. Accessed 18 Oct. 2020.

197 A national network of 61 coordinated task forces representing over 4,500 federal, state, and local law enforcement and prosecutorial agencies. These agencies are continually engaged in proactive and reactive investigations and prosecutions of persons involved in child abuse and exploitation involving the Internet. "Internet Crimes Against Children Task Force Program." www.icactaskforce.org/. Accessed 18 Oct. 2020.

198 US Department of Justice, Federal Bureau of Investigation. "ViCAP" www.fbi.gov/wanted/vicap. Accessed 18 Oct. 2020.

199 US Department of Justice, Federal Bureau of Investigation. "Joint Terrorism Task Forces." www.fbi.gov/investigate/terrorism/joint-terrorism-task-forces. Accessed 18 Oct. 2020.

200 "Secret Service Announces the Creation of the Cyber Fraud Task Force." Press Release, US Secret Service, 9 July 2020, secretservice.gov/data/press/releases/2020/20-JUL/Secret-Service-Cyber-Fraud-Task-Force-Press-Release.pdf. Accessed 18 Oct. 2020.

201 US Department of Justice, Office of the Inspector General. "Audit of the Federal Bureau of Investigation's Implementation of Its Next Generation Cyber Initiative." Jul 2015, oig.justice.gov/reports/2015/a1529.pdf. Accessed 18 Oct. 2020.

202 "Appointment of Christopher Painter as Coordinator for Cyber Issues." Media Note, US Department of State (Archived Content), 21 Apr. 2011, 2009-2017.state.gov/r/pa/prs/ps/2011/04/161485.htm. Accessed 18 Oct. 2020.

203 This should be done in compliance with restrictions on the number of Assistant Secretaries that have been authorized by Congress. See Subsection (c) (1) of 22 USC 2651a. United States Congress. United States Code. Tittle 22, Chapter 38, Section 2651a, Organization of the Department of State. House.gov, uscode.house.gov/view.xhtml?req=(title:22%20section:2651a%20edition:prelim). Accessed 18 Oct. 2020.

204 See, for example, Section 103 of the Department of State Authorities Act of Fiscal Year 2017, mandating that "[t]he Assistant Secretary for Diplomatic Security shall report directly to the Secretary, without being required to obtain the approval or concurrence of any other official of the Department, as threats and circumstances require." United States, Congress, Senate. Department of State Authorities Act, Fiscal Year 2017. Congress.gov, www.congress.gov/bill/114th-congress/senate-bill/1635/text. 114th Congress, 2nd session, S.1635, passed 16 Dec. 2016. Accessed 18 Oct. 2020.

205 United States, Congress, Senate. Cyber Diplomacy Act of 2019. Congress.gov, https://www.congress.gov/bill/116th-congress/house-bill/739. 116th Congress, 1st session, H.R. 739. Accessed 20 Oct. 2020.

206 See, for example, the June 2020 report of the Government Accountability Office for the latest data. Bair, Jason. "State Department: Additional Steps Are Needed to Identify Barriers to Workforce Diversity." Testimony Before the House of Representatives, Committee on Foreign Affairs, Subcommittee on

Oversight and Investigations, 17 June 2020, www.gao.gov/assets/710/707658.pdf. Accessed 18 Oct. 2020.

207 This recommendation does not propose that these individuals be detailees placed in the Office itself, but that they serve as the principal focal point to the Office for their entity.

208 This should exclude funding spent on DOS's internal IT and cybersecurity infrastructure, related personnel, and any other spending related to protecting and securing DOS's own cyber assets.

209 This includes the number of countries, economies, and/or regional organizations with which DOS has new or sustained engagement on cyber issues and the number of enhanced diplomatic engagements facilitated by the Department on cyber issues. US Department of State, Agency for International Development. "FY 2018 Annual Performance Report and FY 2020 Annual Performance Plan." www.state.gov/wp-content/uploads/2019/05/FY-2020-Annual-Performance-Plan-and-FY-2018-Annual-Performance-Report.pdf. Accessed 18 Oct. 2020.

210 US Department of State, Office of the Coordinator for Cyber Issues. "Recommendations to the President on Protecting American Cyber Interests through International Engagement." 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 27 Oct. 2020.

211 This could include, for example, sponsoring an Arria-formula meeting at the UN Security Council on cybercrime.

212 Council of Europe. "Budapest Convention and related standards." www.coe.int/en/web/cybercrime/the-budapest-convention. Accessed 18 Oct. 2020.

213 In evaluating models for this private sector engagement, DOS could look to models developed by international organizations such as the International Telecommunication Union in order to create a formal entity at the Department to allow for regular, transparent consultation and trust-building.

214 Paris Call. "The Paris Call for Trust and Security in Cyberspace." 2018, pariscall.international/en/. Accessed 18 Oct. 2020.

215 Global Commission on the Stability of Cyberspace. "The Rules of the Road: GCSC Proposed Norms of Responsible Behavior in Cyberspace." https://cyberstability.org/norms/. Accessed 18 Oct. 2020.

216 See recommendation 6 on the establishment of a multistakeholder engagement mechanism. Global Commission on the Stability of Cyberspace. "Advancing Cyberstability: Final Report." Nov. 2019, cyberstability.org/report/#7-recommendations. Accessed 18 Oct. 2020.

217 US Department of State, Agency for International Development. "Enduring Leadership in a Dynamic World." Quadrennial Diplomacy and Development Review, 2015, p. 84. 2012–2017. usaid.gov/sites/default/files/documents/1870/QDDR2015.pdf. Accessed 18 Oct. 2020.

218 The last QDDR was conducted in 2015 by the Obama Administration. US Department of State, Agency for International Development. "Enduring Leadership in a Dynamic World." Quadrennial Diplomacy and Development Review, 2015, p. 84. 2012-2017.usaid.gov/sites/default/files/documents/1870/QDDR2015.pdf. Accessed 18 Oct. 2020.

219 US Department of State, Agency for International Development. "Leading Through Civilian Power." Quadrennial Diplomacy and Development Review, 2010, pp. 45-48. 2009-2017. state.gov/documents/organization/153108.pdf. Accessed 18 Oct. 2020.

220 Including those under the April 2015 Executive Order 13694 and December 2016 Executive Order 13757; cyber sanctions contained in the International Emergency Economic Powers Act (IEEPA, 50 USC §§ 1701–1706), National Emergencies Act (NEW, 50 USC §§ 1601–1651), and the "Countering America's Adversaries Through Sanctions Act" (P.L. 115-44) (CAATSA); and country-specific sanctions regimes such as those for North Korea, Iran, Syria, and Ukraine-/Russia-related activities. US Department of State. "Cyber Sanctions." www.state.gov/cyber-sanctions/. Accessed 18 Oct. 2020; US Department of the Treasury. "Sanctions Programs and Country Information." home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information. Accessed 18 Oct. 2020.

221 Logan, Trevor and Patel, Pavak. "Data Visualization: U.S. Sanctions Against Malicious Cyber Actors." Foundation for Defense of Democracies, 20 Apr. 2020, www.fdd.org/analysis/visuals/2020/02/28/data-visualization%3A-us-sanctions-against-malicious-cyber-actors/. Accessed 18 Oct. 2020.

222 Thompson, Natalie, "Targeted Financial Sanctions and Countering Malicious Cyber Activity," Carnegie Endowment for International Peace, forthcoming.

223 Botek, Adam. "European Union establishes a sanction regime for cyber-attacks." NATO Cooperative Cyber Defence Centre of Excellence, ccdcoe.org/library/publications/european-union-establishes-a-sanction-regime-for-cyber-attacks/. Accessed 18 Oct. 2020; "Treasury Sanctions Nigerian Cyber Actors for Targeting U.S. Businesses and Individuals." Press Release, US Department of the Treasury, 16 June 2020, home.treasury.gov/news/press-releases/sm1034. Accessed 18 Oct. 2020; "UK Cyber Sanctions," UK.gov, 18 June 2020, www.gov.uk/government/collections/uk-cyber-sanctions. Accessed 18 Oct. 2020.

224 US Government Accountability Office. "Economic Sanctions: Agencies Assess Impacts on Targets, and Studies Suggest Several Factors Contribute to Sanctions' Effectiveness." 2 Oct. 2019, www.gao.gov/products/GAO-20-145. Accessed 19 Oct. 2020.

225 Support to an FFRDC, in particular, could help eliminate challenges faced by classification restrictions.

226 United Nations. "Countering the use of information and communications technologies for criminal purposes: resolution / adopted by the General Assembly." 2019, digitallibrary.un.org/record/3841023?ln=en. Accessed 18 Oct. 2020.

227 Hakmeh, Joyce and Peters, Allison. "A New UN Cybercrime Treaty? The Way Forward for Supporters of an Open, Free, and Secure Internet." The Council on Foreign Relations, 13 Jan. 2020, www.cfr.org/blog/new-un-cybercrime-treaty-way-forward-supporters-open-free-and-secure-internet. Accessed 18 Oct. 2020.

228 See, for example, section 813(c) of the Department of State Authorization Act of 2019 (H.R. 3352). United States, Congress, House. Department of State Authorization of 2019. Congress.gov, www.congress.gov/bill/116th-congress/house-bill/3352. 116th Congress, 1st session, H.R. 3352. Accessed 18 Oct. 2020.

229 This should be done in accordance with all presidential directives on security assistance.

230 This includes, but is not limited to: programs and technical assistance coordinated and implemented by the State Department's Bureau of International Narcotics and Law Enforcement; programmatic initiatives supported by the Bureaus of Counterterrorism and Countering Violent Extremism and Diplomatic Security; programmatic support provided through the Office of the Coordinator for Cyber Issues (S/CCI); programs implemented by USAID and through all US government development assistance; programs implemented by the Department of Justice's International Criminal Investigative Training Assistance Program (ICITAP), Overseas Prosecutorial Development Assistance and Training (OPDAT), and other DOJ entities; and assistance provided through international organizations.

231 Freedom Online Coalition. "Human Rights Impact of Cybersecurity Laws, Practices and Policies." freedomonlinecoalition.com/wp-content/uploads/2020/02/FOC-Statement-on-Human-Rights-and-Cyber-Security-07.02.pdf. Accessed 19 Oct. 2020.

232 United States, Congress, Senate. Women, Peace, and Security Act of 2017. Congress.gov, www.congress.gov/115/plaws/publ68/PLAW-115publ68.pdf. 115th Congress, 1st session, S. 1141, passed 6 Oct. 2017. Accessed 19 Oct. 2020.

233 See, e.g., US Department of State. "18 FAM 301.1, Managing for Results (MFR) Framework." fam.state.gov/FAM/18FAM/18FAM030101.html. Accessed 19 Oct. 2020.

234 Garcia, Michael and Hindocha, Anisha. "Where Are We Now? Examining the Trump Administration's Efforts to Combat Cybercrime." Third Way, 22 June 2020, www.thirdway.org/report/where-are-we-now-examining-the-trump-administrations-efforts-to-combat-cybercrime. Accessed 19 Oct. 2020.

235 See, e.g., Peters, Allison and Jordan, Amy. "Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime." Journal of National Security Law & Policy, Vol. 10:583, May 2020, p. 516. jnslp.com/wp-content/uploads/2020/05/Countering-the-Cyber-Enforcement-Gap.pdf. Accessed 19 Oct. 2020.

236 Peters, Allison and Jordan, Amy. "Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime." Journal of National Security Law & Policy, Vol. 10:583, May 2020, pp. 490-496. jnslp.com/wp-content/uploads/2020/05/Countering-the-Cyber-Enforcement-Gap.pdf. Accessed 19 Oct. 2020.

237 One assessment published in 2018 mapped over 650 different actors, including government, private sector, and international and non-government organizations, involved in over 50 international and multilateral initiatives in the fight against cybercrime around the globe. Nearly 75 percent of those initiatives were focused on capacity building. This does not include bilateral US capacity building programs. Dupont, Benoît. "Mapping the International Governance of Cybercrime." Governing Cyber Security in Canada, Australia, and the United States, Center for International Governance Innovation, 2018, pp. 23-24. perma.cc/P6CZ-NKND. Accessed 19 Oct. 2020. This includes efforts related to child online protection and combating child exploitation.

238 US Department of Justice, Office of Overseas Prosecutorial Development, Assistance and Training. "Global Cyber and Intellectual Property Crimes." 8 Oct. 2020, www.justice.gov/criminal-opdat/global-cyber-and-intellectual-property-crimes. Accessed 19 Oct. 2020.

239 See, for example, some of the references in Peters, Allison and Jordan, Amy. "Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime." Journal of National Security Law & Policy, Vol. 10:583, May 2020, p. 523. jnslp.com/wp-content/uploads/2020/05/Countering-the-Cyber-Enforcement-Gap.pdf. Accessed 19 Oct. 2020.

240 United States, Congress, House. Consolidated Appropriations Act of 2018. Congress.gov, www.congress.gov/115/plaws/publ141/PLAW-115publ141.pdf, 115th Congress, 2nd session, P.L. 115-141, div. V, passed 23 Mar. 2018. Accessed 19 Oct. 2020.

241 Some surveys of US law enforcement indicate that upward of 80% of criminal cases now involve some form of digital evidence. See Rogers, M., et al. "Survey of Law Enforcement Perceptions Regarding Digital Evidence." IFIP International Federation for Information Processing, Volume 242, Advances in Digital Forensics III; edited by P. Craiger and S. Slienoi, Boston: Springer, 2007, p. 42, https://link.springer.com/chapter/10.1007/978-0-387-73742-3_3. Accessed 19 Oct. 2020.

242 Mulligan, Stephen. "Cross-Border Data Sharing Under the CLOUD Act." Congressional Research Service, 23 Apr. 2018, fas.org/sgp/crs/misc/R45173.pdf. Accessed 19 Oct. 2020. This may continue to shift as more countries take steps toward data localization. See Bowman, Courtney. "Data Localization Laws: An Emerging Global Trend." Jurist.org, 6 Jan. 2017, www.jurist.org/commentary/2017/01/courtney-bowman-data-localization/. Accessed 19 Oct. 2020.

243 US Department of Justice, Criminal Division. "Performance Budget FY 2021 Congressional Submission." p. 9. www.justice.gov/doj/page/file/1246356/download. Accessed 19 Oct. 2020.

244 US Department of Justice. "Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act." April 2019, p. 3, www.justice.gov/dag/page/file/1153436/download. Accessed 19 Oct. 2020.

245 US Department of Justice, Criminal Division. "FY 2016 President's Budget." p. 25, www.justice.gov/sites/default/files/jmd/pages/attachments/2015/02/02/10._criminal_division_crm.pdf. Accessed 19 Oct. 2020.

246 US Department of Justice. "U.S. Department of Justice FY 2019 Budget Request." p. 1. www.justice.gov/file/1033596/download. Accessed 19 Oct. 2020.

247 US Department of Justice, Criminal Division. "Performance Budget FY 2021 Congressional Submission." p. 10. www.justice.gov/doj/page/file/1246356/download. Accessed 19 Oct. 2020.

248 Specifically, the Act authorizes the President to enter into executive agreements with foreign countries that lift the bar on direct disclosures, so long as specified substantive and procedural requirements are met. Once these agreements are in place, the relevant foreign government officials can seek communications content directly from US-based providers without having to go through the MLA system. Conversely, US law enforcement is given the green light to make equivalent, direct requests to the relevant foreign-based entity.

249 Mulligan, Stephen. "Cross-Border Data Sharing Under the CLOUD Act." Congressional Research Service, 23 Apr. 2018, fas.org/sgp/crs/misc/R45173.pdf. Accessed 19 Oct. 2020; US Department of Justice. "Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act." April 2019, p. 3. www.justice.gov/dag/page/file/1153436/download. Accessed 19 Oct. 2020.

250 "Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime." Gov.UK, 3 Oct. 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/836969/CS_USA_6.2019_Agreement_between_the_United_Kingdom_and_the_USA_on_Access_to_Electronic_Data_for_the_Purpose_of_Countering_Serious_Crime.pdf. Accessed 19 Oct. 2020; "Joint Statement Announcing United States and Australian Negotiation of a CLOUD Act Agreement by U.S. Attorney General William Barr and Minister for Home Affairs Peter Dutton." Press Release, US Department of Justice, 7 Oct. 2019, www.justice.gov/opa/pr/joint-statement-announcing-united-states-and-australian-negotiation-cloud-act-agreement-us. Accessed 19 Oct. 2020.

251 United States, Congress, House. Consolidated Appropriations Act of 2018. Congress.gov, www.congress.gov/115/plaws/publ141/PLAW-115publ141.pdf, 115th Congress, 2nd session, P.L. 115-141, div. V, sec 105, passed 23 Mar. 2018. Accessed 19 Oct. 2020.

252 Daskal, Jennifer and Swire, Peter. "Privacy and Civil Liberties Under the CLOUD Act: A Response." Lawfare, 18 Mar. 2018, www.lawfareblog.com/privacy-and-civil-liberties-under-cloud-act-response. Accessed 19 Oct. 2020.

253 US Department of Justice. "Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act." April 2019, p. 3. www.justice.gov/dag/page/file/1153436/download. Accessed 19 Oct. 2020.

254 United States, Congress, House. Consolidated Appropriations Act of 2018. Congress.gov, www.congress.gov/115/plaws/publ141/PLAW-115publ141.pdf, 115th Congress, 2nd session, P.L. 115-141, div. V, sec 103, passed 23 Mar. 2018. Accessed 19 Oct. 2020. For more information on Part 1 of the CLOUD Act, see Mulligan, Stephen. "Cross-Border Data Sharing Under the CLOUD Act." Congressional Research Service, 23 Apr. 2018, fas.org/sgp/crs/misc/R45173.pdf. Accessed 19 Oct. 2020.

255 It is expected to allow countries to seek expedited mutual legal assistance when an emergency exists, allowing the US government to provide for and receive more rapid responses to data requests when there is a significant and imminent risk to the life or safety of people. It is also expected to establish a mechanism for law enforcement in a requesting country to obtain subscriber data directly from service providers in another country without going through mutual legal assistance processes, thereby establishing agreed-upon standards and procedures for such requests. See Daskal, Jennifer and Kennedy-Mayo, DeBrae. "Budapest Convention: What is it and How is it Being Updated?" Cross-Border Data Forum, 2 July 2020, www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it-being-updated/. Accessed 19 Oct. 2020.

256 Daskal, Jennifer and Kennedy-Mayo, DeBrae. "Budapest Convention: What is it and How is it Being Updated?" Cross-Border Data Forum, 2 July 2020, www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it-being-updated/. Accessed 19 Oct. 2020.

257 See, e.g., "UNODC and partners release Practical Guide for Requesting Electronic Evidence Across Borders." Press Release. United Nations, 1 Feb. 2019, www.unodc.org/unodc/en/frontpage/2019/January/unodc-and-partners-release-practical-guide-for-requesting-electronic-evidence-across-boarders.html. Accessed 19 Oct. 2020.

258 US Cyberspace Solarium Commission. "United States of America Cyberspace Solarium Commission Report." March 2020, p. 52. drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view. Accessed 19 Oct. 2020.

259 Rush, Mark and Kephart, Jared. "Lifting the Veil on the MLAT Process: A Guide to Understanding and Responding to MLA Requests." K&L Gates, 20 Jan. 2017, www.klgates.com/Lifting-the-Veil-on-the-

MLAT-Process-A-Guide-to-Understanding-and-Responding-to-MLA-Requests-01-20-2017. Accessed 19 Oct. 2020.

260 This includes FBI Cyber Legal Attaches (ALATs) who work with foreign law enforcement to assist in and share information related to cyber investigations; International Computer Hacking and Intellectual Property (ICHIP) attorney advisors supported by the Departments of Justice and State to build the capacity of foreign law enforcement on cybercrime and IPR; Resident Legal Advisors (RLAs) and Intermittent Legal Advisors (ILAs) who work to provide technical assistance and case mentoring to foreign justice systems to ensure they can investigate and prosecute transnational crime and other security threats; and OIA attaches who work with foreign counterparts on operational matters related to criminal investigations and other key personnel. US Department of Justice, Federal Bureau of Investigation. "FBI Deploys Cyber Experts to Work Directly with Foreign Partners." 26 Oct. 2017, www.fbi.gov/news/stories/fbi-deploys-cyber-experts-to-work-directly-with-foreign-partners. Accessed 19 Oct. 2020; US Department of Justice, Computer Crime and Intellectual Property Section. "Overseas Work." 26 Nov. 2019, www.justice.gov/criminal-ccips/overseas-work. Accessed 29 Oct. 2020; US Department of Justice, Criminal Division, "Office of Overseas Prosecutorial Development, Assistance and Training." www.justice.gov/criminal-opdat. Accessed 19 Oct. 2020; US Department of Justice, Office of International Affairs. "Office of International Affairs." 9 June 2015, www.justice.gov/criminal-oia/office-international-affairs. Accessed 19 Oct. 2020.

261 US Cyberspace Solarium Commission. "United States of America Cyberspace Solarium Commission Report." March 2020, p. 52. drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view. Accessed 19 Oct. 2020.

262 At the time of writing, Congress has pending legislation to create a National Cyber Director (NCD) that would perform similar, but not all, of the duties recommended in this report. The legislation authorizes this position at the Director level but for the purposes of this publication the term "National Cyber Advisor" will be used to refer to this position. See: Section 1132 of the FY 2021 National Defense Authorization Act (H.R. 6395): https://www.congress.gov/116/bills/hr6395/BILLS-116hr6395pcs.pdf.

263 The Secretary should consider appointing the head of such an Office at the rank of Assistant Secretary or higher in compliance with statutory restrictions.