U.S. Department of Justice

U.S. DEPARTMENT OF JUSTICE

DEPUTY ATTORNEY GENERAL LISA O. MONACO

COMPREHENSIVE CYBER REVIEW

JULY 2022

U.S. Department of Justice

Office of the Deputy Attorney General

Washington, DC 20530

July 1, 2022

Dear Madame Deputy Attorney General:

In April 2021, you directed a review of how the Department is addressing challenges posed by escalating cyber threats. Within 120 days of your directive, the review resulted in several initial recommendations. The review continued over the ensuing year, offering additional recommendations, some of which you have publicly announced. The review is now complete and is reflected in its entirety in this report.

The wide-ranging announcements, insights, and recommendations contained in this report reflect the efforts and expertise of multiple components across the Department.

The Criminal Division's Computer Crime and Intellectual Property Section, Child Exploitation and Obscenity Section, Office of International Affairs, Money Laundering and Asset Recovery Section, and Office of Overseas Prosecutorial Development, Assistance, and Training drew on their decades of experience with cyber-related investigations, cases, and outreach as they provided invaluable content for the report.

The National Security Division's Counterintelligence and Export Control Section, Office of Law and Policy, and Counterterrorism Section improved the report by sharing unique perspectives on disrupting national security-related cyber threats.

The Executive Office for United States Attorneys, the United States Attorneys' Offices, and the Federal Bureau of Investigation made critical contributions that reflected the insight of the Department's principal litigators and investigators.

Additionally, the Civil Division's Commercial Litigation Branch, the Civil Rights Division, the Bureau of Justice Assistance, the Office of Violence Against Women, the Office of Justice Programs, and Community Oriented Policing Services provided targeted input regarding cyber-related aspects of their missions.

Finally, in assessing how the Department secures its own data and protects privacy, the report relies on information provided by the Justice Management Division, the Office of the Chief Information Officer, the Data Governance Board, and the Office of Privacy and Civil Liberties.

I offer my sincere thanks to all personnel from across the Department who contributed to this report.

Sincerely,

John P. Carlin
Principal Associate Deputy Attorney General

Table of Contents

EXECUTIVE SUMMARY 1

I. INVESTIGATIONS, PROSECUTIONS, AND OTHER DISRUPTIONS 6
1. Coordination and Deconfliction of Investigations 6
2. Department Tools to Disrupt Cyber Threats 9
3. Specific Areas of Investigation and Enforcement 15

II. PARTNERSHIPS IN COMBATING CYBER THREATS 24
1. Pairing Department Actions with Other U.S. Government Efforts 24
2. International Efforts to Combat Cyber Threats 27
3. State, Local, Tribal, and Territorial Investigative Partnerships 36
4. The Private Sector 38

III. RESILIENCE AGAINST CYBER INCIDENTS AND ATTACKS 44
1. Safer Network Security 45
2. Safer Electronic Communication 49
3. Protocols and Policies for Breach Incidents 51
4. Contractor and Vendor Cybersecurity 52

IV. ADDITIONAL PRIORITIES AND VALUES 56
1. Emerging Technologies 56
2. Improving the Department's Cyber Workforce 61

Appendix A: Notable DOJ Cybercrime Actions (2021) 68

EXECUTIVE SUMMARY

In May 2021, Deputy Attorney General Lisa O. Monaco directed the Department of Justice to conduct a comprehensive review of the Department's cyber-related activities and to develop actionable recommendations to enhance and expand the Department's efforts. This report summarizes the findings from that review. It evaluates many different facets of the Department's cyber capabilities, both "offensive" (*i.e.*, how it investigates, prosecutes, and combats cyber threats) and "defensive" (*i.e.*, how it protects its own networks from continuous malicious cyber activity). It also evaluates the Department's engagement with various governmental and private-sector partners; its preparation for emerging technologies; and the ways in which it is building and retaining its cyber workforce for the future.

As stated in the memorandum announcing the review,[i] the focus has been on actionable recommendations to enhance and expand the Department's efforts against fast-changing cyber threats. To that end, the review has already made a number of interim recommendations that Department leadership has accepted and implemented. These include:

- The creation of the **National Cryptocurrency Enforcement Team (NCET)** within the Department's Criminal Division, which focuses on combating illicit uses of cryptocurrency.

- The launch of the **Civil Cyber-Fraud Initiative (CCFI)** by the Department's Civil Division. The CCFI uses the Department's authorities under the False Claims Act to pursue civil actions against government grantees and contractors—including those under contract with the Department of Justice—who fail to meet cybersecurity obligations.

- The development of a new **Cyber Fellowship** within the Department, designed to foster a new generation of prosecutors and attorneys equipped to handle emerging cybercrime and cyber-based national security threats.

- The rollout of additional cybersecurity measures designed to improve the Department's email security. These measures included mandatory Department-wide encryption training for Department personnel and additional technical measures to protect against phishing and related techniques.

Disruption, Accountability, and Deterrence

The threats in cyberspace evolve with unmatched speed. For the Department to disrupt these attacks and hold accountable those responsible, it will need to move with almost unprecedented agility. This past year has shown the Department moving to keep pace with evolving cyber threats. For example, even before the series of significant ransomware attacks during 2021, the Department began to accelerate its focus on the threat through the creation of the **Ransomware and Digital Extortion Task Force.** Today, the Department is investigating over 100 different ransomware variants and ransomware groups that have caused billions of dollars in damage. The Department also had

some notable successes in the last year, including the recovery of approximately $2.3 million in ransom paid to the Colonial Pipeline attackers; the recovery of ransom keys that the Department used to assist victims of the Kaseya ransomware attack; and the arrests of multiple individuals suspected of being involved in these and other significant attacks.

The Department has also quickly adapted to the continued threat of cryptocurrency's illicit uses. While the Department for years has traced cryptocurrency in investigations and combated money laundering involving cryptocurrency, in the last year it has taken additional steps to strengthen its institutional expertise on digital currency. The newly created NCET is now staffed with a Director and more than a dozen prosecutors with backgrounds in money laundering, computer crimes, regulatory policy, forfeiture, and other relevant areas. Additionally, the FBI has created the **Virtual Asset Unit** (VAU), a new partnership between the FBI's Criminal Investigative and Cyber Divisions that will merge their respective expertise in cryptocurrency.

The Department continues to play a unique and critical role in addressing almost every cyber threat. And as many recent examples show, the Department can be impactful against these threats even before prosecution and arrest. Last year saw the Department successfully deploy a number of novel means of disrupting threats, including the seizure of ransomware payments (including the aforementioned Colonial Pipeline seizure) and the court-authorized removal of malware from hundreds of infected computers. These successes should serve as "proof of concept" and renew the Department's commitment to using its full suite of tools to disrupt cyber threats.

One point of emphasis to come out of this review, however, is that the Department can significantly amplify its own efforts by working more closely with its partners and allies—those elsewhere in the U.S. Government; those in like-minded nations; those in state, local, tribal, and territorial governments; and those in the private sector. Given the transnational nature of significant cyber threats—and the fact that many are state-sponsored or state-sanctioned—the Department needs to couple its own tools with those of its partners.

For this reason, the Department will designate an experienced Department prosecutor to serve as the first-ever **Cyber Operations International Liaison (COIL)**, whose responsibility will be to work with applicable Department components and European allies to increase the tempo of or otherwise enable operations and other disruptive actions against top-tier cyber actors, including charges, arrests, extraditions, asset seizures, and the dismantlement of infrastructure.

The Department has a proven track record of working with these partners, but it can further improve its coordination, including through some recommendations proposed in this report. One recommendation is to require all prosecutors handling significant cyber investigations with transnational links to consult with attorneys in the Department's Criminal Division (CRM) and National Security Division (NSD) who have experience and training in working with the relevant partners to ensure a multi-front response to an ongoing threat. Another recommendation is to continue to assign Department personnel to other Departments that have different authorities and tools; based on a recommendation during this review, for example, a Department attorney for the first time was seconded to the Defense Department's Cyber Command in an effort to increase interagency partnerships. The collective goal of these recommendations is to ensure that the Department's thinking about whole-of-government and international campaigns is more proactive and begins as early as possible in an investigation.

Strengthening the Department's Defenses and Building Resilience

While the Department plays a key role in defending others from malicious cyber activity, it must also ensure that its networks and systems are properly defended from a continuous barrage of state-sponsored and criminal attacks. Since the December 2020 breach linked to the global SolarWinds supply-chain compromise and related breaches of Microsoft Office 365 (O365) systems, the Department has redoubled its efforts to remediate against that intrusion and protect against another significant compromise.

The Department's own internal review of its preparedness coincided with the issuance of "Executive Order on Improving the Nation's Cybersecurity" (E.O. 14028), which sets forth new measures that all federal departments and agencies must take to improve the U.S. Government's collective cybersecurity. This review's assessment of the Department's "cyber-defenses" focused on how the Department could better follow the directives set forth in E.O. 14028, including specific multi-factor authentication, data-at-rest encryption, logging, and cloud computing standards. However, a number of additional areas were flagged as areas where the Department could improve its practices in order to increase its cybersecurity. These included the Department's electronic communications practices (including email and document-transfer practices), mobile device security, and contractor cybersecurity requirements. For each area identified, this report recommends steps to avoid unnecessary exposure to another significant cyber incident.

The review also concluded that the Department would benefit from updated response plans to a significant cyber intrusion into its own systems. The review found, for example, that the existing policies for the information security team had not been updated to include the lessons learned from the December 2020 breach. The review also concluded that planning should not just be limited to information security personnel and privacy officers, but rather involve the leadership of all offices and divisions within the Department. To that end, the review recommended that separate cyber-incident response materials (called the **Justice Cyber Incident Playbook**) be prepared for the Department's leadership, so that the response to cyber incidents will involve those who understand the operational significance of a breach and can direct relevant personnel to take remedial actions.

Ensuring Policies and Workforce Reflect the Department's Priorities and Values

This review considered two other important sets of issues that will be critical as the Department positions itself for the future: how it will deal with emerging technologies, and what can be done to ensure the Department has a qualified and supported workforce.

Many offices and divisions within the Department already spend significant time and effort identifying the impact of new technologies, considering their impact on civil liberties, public safety, competition, or the Department's own investigative capabilities. Too often, however, these efforts to evaluate technologies are siloed, such that the cross-cutting expertise across the Department has not been leveraged. To that end, the report focuses on developing ways to take an interdisciplinary approach to evaluating new technologies.

The review recommends that this work start with an **Emerging Technology Board**, whose responsibility will be to ensure that the

Department evaluates the implications of new technology by enlisting the diverse expertise across the Department. This Board will help coordinate disparate efforts to avoid duplication, as well as ensure that all stakeholders within the Department have a chance to consider these important issues.

When it comes to its own use of these technologies, the Department also needs to ensure that it has appropriate frameworks in place to avoid misuse of new technologies. Based on a recommendation from this review, for example, the Department recently completed the **Principles for the Ethical Use of Artificial Intelligence**, which will serve as a way for the Department to ensure that artificial intelligence is deployed appropriately, whether assisting in personnel decisions or identifying suspects in an investigation. The report identifies other areas for similar focus in the future.

Finally, the report considers ways in which the Department can build its cyber workforce for the future. Whether a systems engineer, cyber prosecutor, cyber policy expert, special agent, or analyst, Department employees are talented and will continue to receive job offers from other agencies and the private sector. The risk of personnel attrition is heightened by the fact that other departments within the U.S. Government have recently begun to offer more competitive salaries to cyber experts. In many cases, hiring offices within the Department do not appear to be aware of similar authorities. As a first step, therefore, the review recommends that hiring offices receive information and instruction on available and under-utilized incentives for some of the most competitive positions.

Note

This report builds on the Department's prior work to address cyber challenges, including the 2018 *Report of the Attorney General's Cyber Digital Task Force and the 2020 Cryptocurrency Enforcement Framework*, and therefore does not repeat many of the overviews of the Department's work or legislative recommendations that have not yet been enacted by Congress. A central goal of the Comprehensive Cyber Review is to identify concrete and actionable ways the Department can draw on the full range of its criminal, civil, national security, and administrative authorities and resources to confront the multidimensional cyber challenge. Many of the recommendations contained in this report reflect practices and efforts already underway within the Department, led by career attorneys, agents, analysts, and others, and reflect lessons learned in numerous individual cases.

I. INVESTIGATIONS, PROSECUTIONS, AND OTHER DISRUPTIONS

The Department of Justice's core priority is to keep the country and its people safe from all threats, foreign and domestic. As Attorney General Garland stated, "Cybercrime is a serious threat to the country: to our personal safety, to the health of our economy, and to our national security."[ii] The Department has been at the forefront of fighting cyber and cyber-enabled crimes since their inception. Today, the Department serves as the lead federal agency for threat response activities. In that role, the Department as a whole addresses the many and diverse threats posed by cybercriminals, ranging from malicious cyber actors in pursuit of personal profit to nation-state cyber actors who seek to undermine security and democratic processes.

Cybercriminals victimize individuals, businesses, organizations, and government entities throughout the United States. They can act as lone hackers, as members of transnational criminal organizations, or work for or at the direction of nation-state adversaries. They conduct their crimes both by employing infrastructures built for and marketed to criminal actors, as well as by abusing legitimate digital and financial infrastructure. Cybercriminals pose a constantly evolving threat, as they strive to exploit new technologies and techniques in furtherance of their malicious activities.

The Department plays a critical role in identifying those who engage in cyber and cyber-enabled crimes, holding cybercriminals responsible, disrupting their capacity to carry out attacks, frustrating their efforts to profit from their crimes, and otherwise deterring similar future conduct. To ensure the Department is best positioned to meet the cyber challenge, it must make sure that its efforts across its components are properly focused, resourced, and coordinated. To do so, it must (1) make data-driven decisions about investigations to prioritize threats and ensure coordination and deconfliction across the Department's efforts; (2) address the entirety of the criminal ecosystem that allows criminals to flourish and persist, including the malicious actors, state sponsors, technology, and tools that aid and enable cybercriminal activity; and (3) ensure that all available tools are used to combat cyber threats, and develop new tools that account for the fast-evolving nature of the threat.

> *"[The cyber threat] has exploded. It has become more diffuse, more sophisticated, more dangerous than ever before."*
>
> Deputy Attorney General (DAG) Lisa O. Monaco, Address at Annual Munich Cybersecurity Conference (Feb. 17, 2021)

1. Coordination and Deconfliction of Investigations

The nature of the cyber threat is varied, persistent, and widespread. In many instances, cybercriminals are located overseas, prey on numerous victims in districts across the United States, and rely on decentralized structures involving many actors who may not know one another's real identities or locations.

Through its headquarters experts, 94 U.S. Attorneys' Offices, 56 FBI field offices, and other personnel, the Department of Justice has unparalleled domestic reach. One result is that

a cybercriminal group may be responsible for a series of attacks that harm victims located in the areas of responsibility for dozens of different districts and field offices. Additionally, any one cybercriminal actor or group may be involved in any number of different criminal activities. Given this diffuse nature of cybercriminal organizations and the breadth of the conspiracies, multiple components may be investigating related cybercriminal groups at the same time.

To ensure that the Department of Justice has the greatest disruptive impact possible, its prosecutors, agents, analysts, and other personnel must be coordinated, efficiently sharing information and allocating their efforts and resources to best address these threats. Close coordination on cybercriminal investigations across the Department is crucial to meeting its goal of criminally prosecuting or otherwise disrupting those responsible and protecting the public health, safety, and national security. At a minimum, uncoordinated investigations threaten to waste Department time and resources with duplicative efforts; erode relationships with companies and foreign partners responding to redundant requests; and harm Department morale. In certain instances, a lack of coordination could potentially hamper investigations and prosecutions through, for instance, inconsistent investigative efforts, loss of opportunity to take essential investigative steps due to a lack of sharing of crucial evidence across case teams, and the possible exposure of classified or sensitive operations or information. In addition, as cybercriminals continue to evolve in this area, it is important that the Department apply its authorities as well as bring charges in a consistent manner across all components and investigations.

Data-Driven Prioritization of Threats: The Department of Justice, including the FBI, is situated at the crossroads of the law enforcement and intelligence communities. Through its investigations across multiple components and its relationships with other agencies, departments, the private sector, and international partners, the Department possesses a wealth of threat intelligence regarding cyber and cyber-enabled threats. The Department must ensure that it is leveraging this data to develop a comprehensive picture of the cyber threat landscape and is prioritizing those individuals and organizations that pose the most severe cyber threats to the nation.

The Department, acting primarily through the FBI and the National Cyber Investigative Joint Task Force (NCIJTF) (*see* p. 27), should prioritize its efforts to identify crucial ties and relationships across national and global investigations and cases to ensure that case teams can follow and leverage all available investigative leads. The Department should also comprehensively assess its information holdings to identify those criminal targets—such as recidivist cyber actors engaging in a variety of different criminal schemes; prolific ransomware actors who use multiple ransomware variants for their attacks; and online criminal infrastructure used by different criminal groups—that should be prioritized for investigative and prosecutorial resources.

Once threats are prioritized, the FBI and NCIJTF should ensure that others in the Department, as well as partners outside the Department (discussed further in Part II), receive information resulting from this prioritization. Sharing this information will ensure that this effort can inform the prioritization and coordination of efforts across partners against the myriad cyber threats.

Expanded Tracking of Cyber Investigations: In June 2021, the Deputy Attorney General issued a Memorandum directed at all federal

prosecutors providing for increased reporting related to cases involving ransomware and digital extortion (hereinafter the "Reporting Memorandum").[iii] As explained in the Reporting Memorandum, tracking investigations across the Department is necessary "[t]o ensure we can make necessary connections across national and global cases and investigations, and to allow us to develop a comprehensive picture of the national and economic security threats we face."[iv] Under the Reporting Memorandum requirements, all prosecutors handling ransomware and ransomware-related investigations are required to report such investigations and major developments therein to CRM's Computer Crime and Intellectual Property Section (CCIPS) and the National Security & Cyber Crime Coordinator for the Executive Office of the United States Attorneys (EOUSA).[v] The Reporting Memorandum also designated CCIPS to be responsible for coordinating all ransomware and related cases, in some instances alongside other Department components.

The same concerns that were identified in the Reporting Memorandum for ransomware and digital extortion apply to a number of transnational cyber threats, including significant hacking conspiracies, illicit darknet marketplaces, and cryptocurrency-enabled money laundering operations. The Department should therefore build on the reporting requirements set forth in the Reporting Memorandum and extend them to significant transnational cyber investigations. Specifically, the Department should consider requiring prosecuting offices to report open investigations into unauthorized hacking into a computer system; transmission of malware; counter antivirus services; illicit darknet markets; botnets; bulletproof hosting services; and illicit online money laundering services.

A broader reporting model would provide the Department with a more comprehensive understanding of other significant cyber threats and ensure that its investigations into cyber and cyber-enabled criminal behavior impacting multiple districts are well-coordinated across the Department. Further, Department leadership can use the data collected under this reporting requirement to make resource decisions and identify areas for further prioritization.

Deconfliction of Cyber Investigations and Prosecutions: In an effort to better resource investigations and avoid unnecessary duplication, the Department should also issue a policy to ensure that prosecutors and agents take steps at the investigative stage to facilitate early coordination and deconfliction in cases in which multiple offices and law enforcement agencies are investigating related cybercriminal actors or conduct. The policy should emphasize a "One Department" approach to addressing related cyber threats and discourage traditional turf wars among components and offices, thus decreasing redundant and inconsistent investigative and prosecutorial efforts.

Additionally, the Department should establish deconfliction procedures that account for the multitude of law enforcement agencies involved. Federal prosecutors partner with a variety of law enforcement agencies outside the Department in investigating cyber and cyber-enabled cases, including the U.S. Secret Service, Homeland Security Investigations, Internal Revenue Service-Criminal Investigation, and state and local prosecutors. Such partnerships are valuable given the extensive nature of these attacks and the limited resources of the Department. However, the introduction of additional law enforcement agencies requires additional coordination within the Department to avoid unnecessary duplication of efforts that are inefficient or counterproductive. To that end, in conjunction with the new reporting requirements discussed above, the Department should issue

a policy requiring prosecutors who open a cyber investigation with a law enforcement partner besides the FBI to ensure that proper deconfliction has occurred. In issuing this guidance, the Department should coordinate with its law enforcement partners to identify the best mechanism for such deconfliction, including consideration of a requirement that prosecutors ensure that their local FBI field office and NCIJTF are notified of new investigations. Through this policy, the Department can ensure that it does not duplicate efforts by opening cases on threats already being investigated by another law enforcement agency.

2. Department Tools to Disrupt Cyber Threats

Unique among the Department of Justice's authorities is the ability to hold criminal actors accountable through arrests and prosecutions. It is the hallmark of the work that the Department pursues across a wide range of crimes, and it is similarly effective in preventing future cyber threats. Cybercrime, however, poses challenges in this regard: cybercriminals employ a variety of methods to evade detection and identification, sometimes acting in countries that turn a blind eye to the crimes, or even authorize, support, or direct their activities while not expressly sponsoring them. In other instances, the cybercriminals are themselves members of a foreign intelligence or military service.

The Department of Justice's ability to combat cyber threats, however, is not limited to arresting and prosecuting the individual operators behind the keyboard. In recent years, the Department has increasingly developed other tools to remedy vulnerabilities and disrupt vectors for attack, to change the risk-reward calculus by imposing consequences and otherwise increasing the costs for cybercriminals, and to assist victims of cyberattacks.

> *"My message to the department is clear: we should be looking for success both inside and outside the courtroom."*
>
> DAG Lisa O. Monaco, Address at Annual Munich Cybersecurity Conference (Apr. 20, 2022)

As in all criminal cases, charging and apprehending actors to hold them responsible for their actions is a priority in cybercrime cases. However, efforts to address the threat that these actors pose also include disrupting their ongoing criminal activities and the ways in which they seek to monetize or otherwise leverage their activities.[vi] These disruptive actions should continue and expand to incorporate all available criminal, civil, national security, and administrative tools to dismantle the infrastructure used by cybercriminals, as well as to deprive malicious actors of the fruits of their criminal actions, including through seizures and forfeitures of property derived from or involved in the criminal activity wherever possible. Investigators and attorneys should also assess, at each stage of the investigation, whether there are other impactful actions aside from apprehension of the actors in question that may be taken to remedy or minimize the ongoing risk of harm.

Disruptive actions that Department personnel should consider include: (1) seizures and searches of domains, command-and-control (C2) servers, and other infrastructure owned or operated by criminals; (2) use of court-authorized orders to remove or disrupt malicious software so as to prevent additional attacks and harm to victims; and (3) freezing, seizing, and forfeiting property derived from or involved in criminal activity. If opportunities to take

such disruptive actions arise over the course of an investigation, attorneys and agents should carefully consider whether taking such actions could mitigate ongoing harm posed by the actors, such as by changing their risk-reward calculus, by otherwise protecting victims, or by making victims whole after having suffered an attack. Impactful operations that bring substantial or significant disruptions of criminal cyber activity should be pursued, even if such actions might otherwise alert criminal actors of the nature or existence of the Department's investigation and thus make apprehension of individual actors over the short term more challenging.

Recent examples of instances in which the Department has worked to take disruptive action against cybercriminal actors and infrastructure include:

- Seizure of Proceeds from a Ransomware Attack: In June 2021, the Department of Justice announced that, pursuant to a court-issued seizure warrant, the Department of Justice had seized $2.3 million in bitcoin that represented proceeds of a ransom payment made to individuals in the DarkSide ransomware group. The ransomware payment was made in connection with an attack on Colonial Pipeline—the largest pipeline system for refined oil products in the United States—that forced Colonial to temporarily suspend operations.[vii]

- Removal of Malware from a Victim Computer: In April 2021, the Department obtained court authorization to copy and remove malicious web shells from hundreds of vulnerable computers used to provide enterprise-level email service. These web shells had been previously placed on the infected computers using a zero-day vulnerability in Microsoft Exchange Server software.[viii]

- Seizure of Domain Names Used in Spear-Phishing Campaign: In June 2021, the Department announced a court-authorized operation to seize two domains used in spear-phishing activity that mimicked email communications from USAID.[ixx]

In addition, the Department has demonstrated its capabilities to disrupt cybercriminal threats through its efforts against the Emotet botnet (*see* p. 28); the Sodinokibi/REvil ransomware group (*see* p. 35); the Lazarus group (*see* p. 14); and APT41 (see p. 16).[xi]

Figure 1 – Deputy Attorney General Lisa O. Monaco at Press Conference Regarding Disruption and Prosecution of Russian Malign Activity, April 6, 2022.

"There is no higher priority at the Department than using all available tools to protect our nation, including from ransomware and other digital threats."

DAG Lisa O. Monaco, Press Conference on Darkside Attack on Colonial Pipeline (Jun. 7, 2021)

Determining the panoply of available tools and operations requires extensive coordination among Department attorneys, the investigative agencies, and technical experts at the Department. The Department should ensure that attorneys, agents, analysts, and others are trained on the newest developments and disruption techniques, including through the Computer Hacking and Intellectual Property (CHIP) and National Security Cyber Specialist (NSCS) networks. In order to signal the priority of disruptive actions, the Department should also ensure it recognizes and rewards cyber disruption activities that do not end with a defendant in a federal courtroom, given that non-prosecutorial activities can be incredibly impactful to protecting personal, economic, and national security.

As new opportunities and tools arise, continuous intradepartmental communication should continue to ensure that legal obligations, effects on privacy, and law enforcement goals are weighed carefully and that all potential safeguards are considered and employed. (To the extent that these tools rely on emerging technologies, additional recommendations appear in Part IV of this report.) Additionally, when a proposed operation has implications for the intersection between the Department's criminal, national security, and international affairs work, the appropriate attorneys in the Department should be consulted.

A. Addressing the Blended Threat

Crucial to the Department of Justice's efforts in the cyber context is the work done by CRM and NSD in investigating malicious cyber and cyber-enabled activities. But today's cyber threat cannot be neatly addressed by the traditional taxonomy of identifying threats as primarily "criminal" or "national security" in nature. Criminal actors and nation states are forming alliances of convenience, alliances of opportunity, and sometimes alliances by design. Today, some nation states allow this criminal activity to persist without consequence—if not expressly condoning activity within its borders—by acting as a safe harbor for these cybercriminals and turning a blind eye. And the consequences of cyberattacks perpetrated by criminal actors can have national security implications. Instances of this blended threat are as follows:

- *The National Security Threat Posed by Ransomware Attacks:* Malicious cybercriminal actors, many of which are linked to transnational organized criminal groups based in Russia and Eastern Europe, deploy ransomware and digital extortion attacks against U.S. businesses and organizations for profit. In recent years, ransomware attacks have increased in scale, prevalence, and consequence, as attackers increasingly target organizations that can least afford a disruption in services—targets such as critical infrastructure networks that govern a country's pipelines, food supply, hospitals, emergency services, and schools. When a ransomware attack disrupts or threatens the operations of a significant critical infrastructure organization, it has national security ramifications.

- *Cybercrime as Means to Generate Income for Malicious Foreign Governments*: The Department has seen a rise in hackers

with nation-state ties using cybercrime as a way to generate income that can be funneled into other national security threats. For example, in February 2021, the Department unsealed an indictment against three North Korean hackers for participating in a campaign of cyber heists and extortion schemes targeting over $1.3 billion of money and cryptocurrency from financial institutions and companies for the benefit of the North Korean government (*see* p. 14).[xii]

- *Foreign Governments Providing Safe Haven to Hackers:* Over the last decade, the Department's investigations have on multiple occasions publicly exposed state-sponsored hackers, both employees of intelligence services as well as criminal proxies, targeting the United States' and allies' interests. These malicious actors have often "moonlighted" by engaging in hacks for personal profit alongside those designed to advance their home countries' strategic interests.[xiii]

- *Nation-State Techniques Used by Criminal Actors:* Techniques developed by nation-state actors can subsequently be used by criminal actors for their own purposes. For example, in March 2021, Microsoft announced it had identified what it described as nation-state cyber intrusions by a group it called "Hafnium."[xiv] After the state-sponsored threat was discovered and the relevant patches released, the private sector warned about criminal groups moving quickly to take advantage of any unpatched systems.

Given that the diverse scope of cybercriminal activity lies on a spectrum between criminal and national security threats, the Department works to harness its collective resources and expertise to address the blended threat posed by cybercrime. CRM and NSD, as well as the nationwide CHIP and NSCS networks of federal prosecutors, should continue to work collectively on significant cyber intrusion investigations into blended threats. Likewise, the FBI's Cyber Division (CyD) employs a variety of personnel with criminal, counterespionage, and other national security backgrounds to ensure a multidisciplinary approach to studying emerging and persistent threats.

The Department should continue to find ways to foster multidisciplinary approaches to cyber investigations—for example, to ensure CRM prosecutors fully appreciate the national security dimensions of their investigations, and for NSD prosecutors to anticipate the follow-on criminal activity that a state-sponsored intrusion may cause. Ultimately, cyber prosecutors should be familiar with both the national security tools and the traditional criminal enforcement tools relevant to cyber investigations.

> *"[T]he criminal groups and the threats that they pose now have a national security overlay, they have clear national security implications."*
>
> DAG Lisa O. Monaco, Address at Criminal Division Cybersecurity Roundtable: The Evolving Cyber Threat Landscape (Oct. 20, 2021)

Another way to eliminate the wall between "national security" and "criminal" cyber investigations is for personnel who do not specialize in national security investigations to nevertheless proactively work with national security counterparts to identify classified intelligence about a target.[xv] Prosecutors, agents, and analysts should work over the course of an investigation to identify and proactively follow all potential leads, including within the FBI or

other U.S. intelligence community classified holdings, in their efforts to obtain evidence regarding attribution, modus operandi, and any ongoing activities that may lead to future attacks. Where such leads are identified in classified holdings, prosecutors should engage with the applicable NSD component to help facilitate their use of such leads. Similarly, in all cases where there are indications that a cybercriminal may be working on behalf of a foreign government's intelligence service or military, prosecutors and agents should immediately engage with NSD to ensure that investigative resources are being devoted to illuminating, exposing, and otherwise disrupting such connections, even in instances where such connections are not necessary to bring criminal charges.

Efforts Against the Lazarus Group

In February 2021, the Department unsealed an indictment of three members of a North Korean military intelligence agency, the Reconnaissance General Bureau (RGB), known to the cybersecurity community as "Lazarus Group" and "Advanced Persistent Threat (APT) 38." The indictment, which expanded on the Department's 2018 charges against one of the defendants for the 2014 attack on Sony Pictures Entertainment and the creation of the WannaCry 2.0 ransomware in 2017,[xvi] charged the defendants with participating in a wide-ranging criminal conspiracy to conduct a series of destructive cyberattacks, to steal and extort more than $1.3 billion of money and cryptocurrency, to create and deploy multiple malicious cryptocurrency applications, and to develop and fraudulently market a blockchain platform. The charges were also accompanied by the Department's seizure of $1.9 million in cryptocurrency stolen by the North Korean hackers from a New York-based financial services company.[xvii]

Throughout the investigation, the Department, often with the assistance of foreign law enforcement partners, proactively provided specific information to domestic and foreign victims with the goals of remediating any intrusion and preventing future intrusions. The Department also collaborated with the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA), the Department of the Treasury, and certain private cybersecurity companies by sharing and analyzing information about the conspiracy's tactics, techniques, and procedures (TTPs). This collaboration resulted in the public release of a joint cybersecurity advisory and malware analysis reports (MARs) regarding North Korean cryptocurrency malware, with the goal of empowering network defenders against the RGB cyber threat.

The Department's disruption efforts extended to the criminal money laundering networks that were helping the RGB "cash out" the fruits of their heists. For example, in September 2021, a Canadian national was sentenced to 140 months in prison for conspiring to launder tens of millions of dollars stolen in various wire and bank fraud schemes, including one of the RGB hacks charged in the February 2021 indictment.[xviii] Ghaleb Alaumary conspired with Ramon Olorunwa Abbas, aka "Ray Hushpuppi," to launder funds from one North Korean-perpetrated heist of a European bank in February 2019. Abbas was charged in a separate case with conspiring to launder hundreds of millions of dollars from various fraud schemes and pleaded guilty in April 2021. He is awaiting sentencing in the Central District of California.

B. Dismantling the Cybercriminal Ecosystem

As cybercriminals continuously modify their sophisticated techniques to conceal their identities and their criminal activities, the Department's efforts to address the cyber challenge must focus not only on the individuals responsible for the cyberattacks, but also on those who enable these cybercriminal actors to flourish or who otherwise enable the proliferation of sophisticated cyber tools among irresponsible actors. As the profitability of cybercrime and the sale of cyber tools and exploits grows, so too does the ecosystem of services and entities dedicated to supporting malicious cyber-enabled activity.

Elements of the criminal ecosystem include:

- Illicit forums, websites, and platforms, including on the darknet, that are used by cybercriminals to communicate with one another, as well as to sell criminal goods and services;

- Hosting and other technology companies that deliberately offer online infrastructure (including Internet Protocol (IP) addresses, servers, virtual private networks, and domain names) to criminals in order to facilitate a variety of cybercrimes, such as by anonymizing the actors' activities;

- Counter antivirus services (CAV) that allow "crypters" to test malicious files, URLs, IP addresses, and domains to ensure that they are not detected by antivirus solutions; and

- Mixing services and tumblers that let criminals hide illicit virtual currency transactions and launder criminal proceeds.

Providers of these services are one cause of the proliferation of sophisticated intrusion capabilities to nation states and cybercriminals. Successful investigations into and disruptions of the criminal infrastructure that is exploited by malicious actors therefore can make a lasting impact on cybercriminal actor groups. Agents and prosecutors should prioritize these investigations and prosecutions.

The Department has previously recognized that successfully disrupting providers of criminal tools can have outsized effects on an existing threat. In the last year alone, the Department has successfully prosecuted criminals who offered "bulletproof hosting" services designed to help criminals avoid searches and seizures of their servers;[xix] the first-ever case against an individual for running a Bitcoin mixing service;[xx] and a foreign national for operating a "crypting" service used to conceal malware from antivirus software.[xxi] Continued investigations and prosecutions of providers of such services can have significant disruptive effect. Additionally, some of these providers may be easier to locate and arrest, even as their customers remain elusive or in parts of the world where arrest or extradition is more difficult.

The commitment to using disruptive techniques to stop cybercriminals should extend to the providers who build the criminal ecosystem. For example, the Department recently participated in a joint international action to take down a VPN provider that marketed itself as a tool for, and was being used in support of, ransomware deployment and other cybercrime activities.[xxii] Disrupting the ecosystem that fosters cybercriminals, however, requires that the Department systematically research and identify capabilities for effecting technical disruption operations. In particular, the Department should take a more comprehensive and systematic approach towards how it develops tools that could be used in disruption operations, including how it decides whether those tools will be made available in unclassified operations.

APT41 Disruption

In September 2020, the Department unsealed three indictments against five Chinese hackers, known to the cybersecurity community as "APT41," and two Malaysian businessmen, for their role in two separate hacking conspiracies affecting over 100 victim entities in the United States and abroad.[xxiii] The victim companies were in a variety of industries, including software and video game development, computer hardware manufacturing, telecommunications, and social media. These intrusions also facilitated the defendants' other criminal schemes, including ransomware and "cryptojacking," *i.e.*, the unauthorized use of victim computers to mine cryptocurrency. Malaysian authorities arrested the Malaysian defendants, and extradition proceedings are underway.

The Department accompanied these charges and arrests with the court-authorized seizure of hundreds of APT41 accounts, servers, domain names, and C2 "dead drop" web pages. The Department executed these seizures in coordination with actions by several private sector companies, which included disabling numerous accounts for violations of the companies' terms of service and Microsoft's development and implementation of technical measures to block APT41 actors from accessing victim computer systems. The Department also publicly released to network defenders an FBI Liaison Alert System (FLASH) report that contained critical, relevant APT41 TTPs.

3. Specific Areas of Investigation and Enforcement

The Department investigates, prosecutes, and disrupts a wide array of cyber and cyber-enabled crimes—from identity theft rings on carder forums to online threats to cyber espionage. A full accounting of this work is beyond the scope of this report. However, the Department has been particularly active in a number of areas, providing significant opportunities for innovation.

A. Ransomware

"Our message to ransomware criminals is clear: If you target victims here, will target you."

DAG Lisa O. Monaco, Press Release Regarding Ukrainian Arrested and Charged with Ransomware Attack on Kaseya (Nov. 8, 2021)

Ransomware is a type of malware used by cyber actors to extort owners of computer systems. Typically, the malware encrypts files on the victim's computer, rendering the files inaccessible, and sends a ransom note demanding payment in exchange for a key or password to decrypt the files. To further coerce victims into paying, some actors also engage in further digital extortion by stealing sensitive information from victims and threatening to leak or sell the victim's data if the payment is not made.

The Department of Justice has been countering the ransomware threat for more than eight years, dating back at least to the 2014 takedown of the GameOver Zeus botnet, which was used to launch Cryptolocker ransomware attacks. However, the nature of the techniques employed by ransomware actors has evolved, and there has been an increase in the scale, scope, and frequency of ransomware attacks.

Ransomware actors have also changed their business model, with developers responsible for creating the malware now offering ransomware-as-a-service ("RaaS"), by licensing the use of the malware to affiliates for a fee. The RaaS model has decreased the barrier to entry for cybercriminals, in that individual affiliates need not have the technical prowess to develop their own ransomware in order to launch attacks.

To combat the growing number of such attacks, in April 2021, the Department of Justice established the Ransomware and Digital Extortion Task Force. As part of the Task Force, CRM's CCIPS, working with the U.S. Attorneys' Offices, prioritizes the disruption, investigation, and prosecution of ransomware and digital extortion activity by tracking and dismantling the development and deployment of malware, identifying the cybercriminals responsible, and holding those individuals accountable for their crimes. The Department, through the Task Force, also strategically targets the ransomware criminal ecosystem as a whole and collaborates with domestic and foreign government agencies as well as private sector partners to combat this significant criminal threat. Recent successes of the Ransomware and Digital Extortion Task Force's efforts include the seizure of the proceeds of the Colonial Pipeline ransomware attack (*see* p. 10) and the announcement of charges, seizures, and an arrest as a result of a whole-of-government campaign against Sodinokibi/REvil (*see* p. 35).

Presently, the Department and the FBI are investigating over 100 variants of ransomware. In total, the subjects being investigated are suspected of causing over $1 billion in losses to victims. While malicious ransomware actors continue to attack businesses and organizations throughout the United States, combating ransomware and digital extortion schemes will continue to be a major priority for the Department.

B. Cryptocurrency and Digital Assets

> *"As the technology advances, so too must the Department evolve with it so that we're poised to root out abuse on these platforms and ensure user confidence in these systems."*
>
> DAG Lisa O. Monaco, Press Release Regarding Announcing National Cryptocurrency Enforcement Team (Oct. 6, 2021)

As innovations in digital asset and distributed ledger technology have grown, so have the capabilities of criminals, terrorists, and nation states to use those technologies for illicit purposes. Some of the central features of these technologies—including decentralized operation and control, anonymity, and the facilitation of financial transactions without intermediaries—may be exploited by criminal actors in ways that pose significant risks to the public. For instance, cybercriminals rely on cryptocurrencies to facilitate their crimes and to extort ransomware payments from victim companies; dark web traffickers use them to buy and sell drugs, malware and other hacking tools, weapons, and other contraband; nation states and terrorist groups deploy them to circumvent U.S. and international sanctions regimes; and money launderers use them to hide criminal proceeds and the identities of those who profit from them. Moreover, digital assets and cryptocurrencies have been used to facilitate crimes, thefts, frauds, and abuse that target the American public.

The Department of Justice has been at the forefront of complex investigations and prosecutions of criminal misuse of digital assets and cryptocurrency since their inception. Over the past decade, as cryptocurrencies and digital assets have increasingly gained credibility and acceptance, the Department has leveraged its criminal, civil, and national security experience to strengthen its capabilities to fight the illicit use

of cryptocurrency and to hold malicious actors responsible for their abuse of these technologies. This includes efforts to take enforcement action against those online entities—such as exchanges, mixers, and tumblers—that enable criminal actors to flourish and profit from the abuse of these technologies, as well as working toward building the Department's capacity to meet the challenge of distributed ledger technologies across its many investigations.

To further these efforts, as is described in further detail below (*see* p. 19), the Department has recently established a National Cryptocurrency Enforcement Team (NCET): a dedicated team of prosecutors drawn from across the Department working toward meeting the evolving challenge posed by digital assets. The NCET includes the attorneys responsible for the Department's recent arrests and seizure of $3.6 billion worth of stolen cryptocurrency linked to the hack of a virtual currency exchange (*see* p. 19). Additionally, the FBI has recently created the Virtual Asset Unit (VAU) to build its own cryptocurrency tracing and investigative tools (*see* p. 20).

Arrests and Seizure of $3.6 Billion Linked to Hack of Virtual Currency Exchange

In February 2022, the Department announced the arrest of two individuals, Ilya Lichtenstein and Heather Morgan, for allegedly having participated in a conspiracy to launder cryptocurrency that was stolen during the 2016 hack of Bitfinex, a virtual currency exchange.[xxiv] In addition, the Department announced that it had seized over 94,000 bitcoin that had been stolen from Bitfinex, valued at the time of the seizure at over $3.6 billion, which represents approximately 80% of the bitcoin stolen from the exchange. This represents the largest cryptocurrency seizure ever by U.S. law enforcement, as well as the largest single financial seizure in the Department's history.

Lichtenstein and Morgan are alleged to have conspired to launder the proceeds of the 119,754 bitcoin that were stolen from Bitfinex's platform after a hacker breached its systems and initiated more than 2,000 transactions. Those unauthorized transactions sent the stolen bitcoin to a digital wallet under Lichtenstein's control. Approximately 25,000 of the stolen bitcoin then were transferred out of Lichtenstein's wallet through a complex labyrinth of transactions to launder the funds, which resulted in some of the stolen funds being deposited into financial accounts under the control of Lichtenstein and Morgan. The remainder of the stolen funds, comprising more than 94,000 bitcoin, remained in the wallet used to receive and store the illegal proceeds of the hack. After the execution of court-authorized search warrants of online accounts controlled by Lichtenstein and Morgan, special agents obtained access to files that contained the private keys required to access that digital wallet. As a result, law enforcement was able to lawfully seize and recover more than 94,000 bitcoin that had been stolen from Bitfinex.

The National Cryptocurrency Enforcement Team

In October 2021, the Deputy Attorney General announced the creation of a National Cryptocurrency Enforcement Team (NCET) to tackle complex investigations and prosecutions of criminal misuses of cryptocurrency, particularly crimes committed by virtual currency exchanges, mixing and tumbling services, and money laundering infrastructure actors. Housed within the CRM, the NCET combines the expertise of Money Laundering and Asset Forfeiture Section (MLARS), CCIPS, and other Department sections with experts detailed from U.S. Attorneys' offices. The team will also assist in tracing and recovering assets lost to fraud and extortion, including cryptocurrency payments to ransomware groups.

The NCET's responsibilities will include investigating and prosecuting cryptocurrency and digital assets cases; developing strategic priorities for investigations and prosecutions involving digital assets; identifying areas for increased investigative and prosecutorial focus; developing and maintaining relationships with federal, state, local, and international law enforcement agencies that investigate and prosecute cryptocurrency cases; working with private industry to combat the illicit use of digital assets; and developing training related to cryptocurrency-related investigations.

The Virtual Asset Unit (VAU) Strategy

Over the last several years, the FBI has tracked the massive growth in complexity and use of virtual assets by illicit actors. To respond to this trend, the FBI's Criminal Investigative Division and CyD have partnered to design an enterprise-wide virtual asset strategy focusing on: (1) securing investigative and analytical expertise; (2) establishing training and education opportunities; and (3) developing innovative solutions and procuring technical tools.

To implement this strategy, in February 2022, the Financial Crimes Section (FCS) established the VAU. The VAU, working closely with the NCET, will focus on strategic case support for investigating illicit use of virtual assets across all FBI programs. The unit will provide training, equipment, field-deployed expertise in blockchain analysis and virtual asset seizure, as well as an innovation team dedicated to remaining ahead of threats posed by rapidly emerging technologies. The VAU will become a technological hub, equipped with robust virtual asset intelligence, tracing, and seizure tools. The unit will develop a full virtual currency analysis and tracing training curriculum, which will be disseminated to the field to ensure a baseline understanding of virtual currencies and assets. Further specialized training will be available for deployable, field office-based subject matter experts.

C. Cyber Espionage and State-Sponsored Destructive Attacks

For decades, cybercriminals have seen cyber-enabled means as an effective and deniable method to steal the fruits of U.S. and international companies' and universities' innovation, and in some cases provide the stolen information to foreign companies, thereby allowing the recipients to skip costly research and development activities. For example, despite bilateral and multilateral commitments otherwise, the Chinese government continues to engage in cyber-enabled economic espionage targeting the innovation of American and international companies for the benefit of PRC companies. In addition to examples described above, in February 2020, a federal grand jury indicted four members of the Chinese military with hacking into the computer systems of the credit reporting agency Equifax and stealing nearly 150 million Americans' personal data and Equifax's valuable trade secrets relating to data compilations and database designs.[xxv] Identifying and disrupting these activities, in some instances with the assistance of international partners, will remain a priority for Department prosecutors and investigators.

Malicious cyber activities are not limited to intrusions aimed at the theft of information or currency. Cybercriminals are also bent on leveraging the internet and technology for disruptive and destructive effect, often for the geopolitical gain of nation-state employers or sponsors. For example, the Lazarus group (*see* p. 14) carried out a disruptive cyberattack on Sony Pictures Entertainment in 2014 and was responsible for programming the WannaCry 2.0 malware that was unleashed upon the world in 2017. The Sony Pictures Entertainment attack, in particular, was motivated by the RGB's desire to stifle free speech that lampooned North Korean leadership.

When possible, the Department will take appropriate action, often with partners, to disrupt such activities before or shortly after cybercriminals undertake them. For example, in April 2022, the Department conducted a court-authorized operation to disrupt a two-tiered global botnet under the control of the GRU, that had infected thousands of network devices.[xxvi] This operation followed on a May 2018 action in which the Department obtained court orders authorizing the FBI to seize a domain that the GRU used as command-and-control infrastructure for a previous global botnet (known as "VPNFilter") of hundreds of thousands of infected home and office routers and other networked devices.[xxvii] As the Department noted when announcing the operations, these disruptions eliminated instrumentalities that the GRU could have used to carry out similar disruptive and destructive attacks.

At the same time, the Department will continue to prosecute the actors responsible for destructive attacks. In October 2020, the Department unsealed criminal charges against six GRU officers for their role in a conspiracy that conducted some of the world's most destructive malware attacks to date, including the 2015 "KillDisk" and 2016 "Industroyer" attacks, which each caused blackouts in Ukraine; the 2017 "NotPetya" attack, which caused billions in losses worldwide; and the 2018 "Olympic Destroyer" attack, which disrupted thousands of computers used to support the 2018 PyeongChang Winter Olympics.[xxviii]

D. Technology-Facilitated Violence and Abuse

As part of its public-safety mission, the Department must continue to protect Americans from malicious actors seeking to use emerging technology as a tool to victimize others in violent and coercive ways. Such conduct includes

cyberstalking, the non-consensual distribution of intimate images, sextortion, doxing, and swatting, among other offenses. The Department currently investigates and prosecutes such offenses through CRM's CCIPS, as well as cyber-specialized prosecutors across the country. Additionally, where federal jurisdiction requirements are met, the Civil Rights Division (CRT) prosecutes bias-motivated online abuses that rise to the level of a true threat, as well as sex trafficking and forced labor offenses, which are increasingly conducted through online activity.

The Department has identified several areas of opportunity to better protect the American people from technology-facilitated violence and abuse. First, as the methodology used to inflict harm evolves, so too must federal statutes. There is no federal statute expressly prohibiting the non-consensual distribution of intimate images, sometimes referred to as "revenge porn," despite the fact that 46 states, Guam, and the District of Columbia have enacted such legislation. The Department recently supported the Stopping Harmful Image Exploitation and Limiting Distribution (SHIELD) Act of 2021, which would prohibit the non-consensual distribution of intimate images.

Second, many instances of technology-facilitated violence are appropriately handled by state, local, tribal, and territorial (SLTT) law enforcement partners. In fact, many victims who begin receiving online abuse tend to report the crime by calling 911 or their local police precincts in the first instance, especially given that the non-digital corollaries (*e.g.*, partner violence, threats) are traditionally investigated by SLTT authorities. However, many SLTT authorities lack appropriate resources and training to pursue these investigations. To bridge this gap, grantmaking components have committed to providing specialized resources and technical assistance. For instance, the Office of Justice Programs (OJP) Bureau of Justice Assistance (BJA), through its National White Collar Crime Center, will adapt its current SLTT cybercrime curriculum to create a unique curriculum specific to technology-facilitated violence and abuse. Additionally, the Department's Community Oriented Policing Services (COPS) office will produce a written resource and guide that summarizes critical investigative measures that SLTT authorities should take in these investigations. Finally, the Office on Violence Against Women (OVW) has committed to providing training materials specific to technology-facilitated abuse through its recently launched Law Enforcement Training and Technical Assistance Consortium (LETTAC), which is the single point of entry for training and technical assistance for all OVW law enforcement grantees.

E. Online Child Sexual Exploitation

With respect to the landscape of modern offenses involving technology-facilitated child sexual exploitation, the scale, complexity, and dangerousness of threats facing children today is unprecedented. The advent of different online platforms and remote storage options with global reach, as well as the proliferation of encryption and anonymizing technology, has complicated the identification, interdiction, and investigation of online child sexual exploitation.

Project Safe Childhood (PSC) is a nationwide initiative to combat the growing epidemic of technology-facilitated child sexual exploitation and abuse launched in May 2006 by the Department of Justice. Led by the U.S. Attorneys' Offices and CRM's Child Exploitation and Obscenity Section (CEOS), Project Safe Childhood marshals federal, state, and local resources to better locate, apprehend, and prosecute individuals who exploit children via the Internet, as well as to identify and rescue

victims. Through Project Safe Childhood, from 2008 to 2019, the number of defendants prosecuted by the Department of Justice for the production of child sexual abuse material near tripled as a result of steady increases each year.[xxix]

CEOS also improves the law enforcement response to crimes against children through training and outreach. Between 2015 and 2019, the annual National Law Enforcement Training on Child Exploitation reached a total of almost 7,300 law enforcement personnel, prosecutors, and other professionals working in the field. In 2020 and 2021, the National Training was converted to a virtual format and reached a total of 4,855 personnel. Each year, the agenda is carefully designed to provide instruction on cutting-edge technological and legal issues concerning online child sexual exploitation and abuse.

In addition to these efforts, the Department also extensively engages with international partners to generate a global response to this global crime. This work includes significant support to the WePROTECT Global Alliance, which seeks to enhance efforts to identify victims, reduce the availability of child sexual abuse materials online, reduce the re-victimization of children, and increase public awareness of the risks posed by children's activities online. This organization is currently supported by more than 98 countries, 52 technology companies, 63 civil-society organizations, and nine international organizations.

F. Malign Foreign Influence

The Department is uniquely positioned to confront the challenge of foreign malign influence, as well as to help foreign partners counter such activities. It does this in two ways: first, operationally, by investigating, prosecuting, or otherwise disrupting unlawful foreign activities, while also assisting other countries in their own investigations and prosecutions; and second, through capacity building, both with regard to rule of law generally, and with respect to countering foreign malign activities in particular.

Recent years have illustrated that foreign malign influence actors seek to leverage the anonymity of the internet to more effectively carry out their campaigns. For example, in November 2021, the Department charged two Iranian nationals for their role in a cyber-enabled disinformation and threat campaign to influence the 2020 U.S. presidential election.[xxx] However, foreign malign influence efforts are not limited to elections. In October 2018, the Department charged six Russian military intelligence officers with international hacking and related influence and disinformation operations. Among the goals of the conspiracy was the publication of information stolen through hacks of anti-doping organizations (*e.g.*, athletes' medical records) to, among other things, undermine, retaliate against, and otherwise delegitimize those organizations' work to publicly expose a Russian state-sponsored athlete doping program. In some cases, the stolen information was released in a manner that did not accurately reflect its original form. As part of its influence and disinformation efforts, Russian military intelligence engaged in a concerted effort to amplify its operation through proactive outreach by e-mail and private messages to approximately 186 reporters.[xxxi]

These disruption efforts reflect the Department's conclusion that, ultimately, one of the most effective ways to counter malign foreign influence operations is to shine a light on the activity and raise awareness of the threat.[xxxii] Such efforts are an important prong of a whole-of-society effort involving collaboration among government at all levels, social media providers

and others in the private sector, political candidates and organizations, and an active and informed citizenry.

G. Domestic Terrorism/Domestic Violent Extremism

The Department has witnessed a sharp rise in domestic terrorism and domestic violent extremism (DVE) cases, with the number of FBI investigations of suspected domestic violent extremists more than doubling in the last year.[xxxiii] The FBI is the lead U.S. law enforcement agency responsible for combating terrorism and coordinates counterterrorism efforts through, among other things, the FBI's Counterterrorism Division (CTD) and the Joint Terrorism Task Forces (JTTFs). Assistant U.S. Attorneys across the country handle a variety of domestic terrorism and DVE cases, in partnership with the NSD's Counterterrorism Section (CTS). In January 2022, the Assistant Attorney General for the National Security Division announced the creation of a specialized Domestic Terrorism Unit within CTS.[xxxiv]

In combating today's domestic terror threats, the Department must confront the internet's omnipresent role. The internet, for example, serves as the typical means by which lone DVE actors radicalize.[xxxv] As noted in the first-ever *National Strategy on Countering Domestic Terrorism*, released by the White House in June 2021, "[t]hese [recruitment] activities are increasingly happening on Internet-based communications platforms, including social media, online gaming platforms, file-upload sites, and end-to-end encrypted chat platforms."[xxxvi] Separately, the increasing use of encrypted and ephemeral means of online communication also poses difficulties to the Department's counterterrorism efforts, as it does to the Department's work on all cyber-enabled crime.[xxxvii] In certain cases, the internet also facilitates international linkages between many domestic violent extremists.[xxxviii]

In addition to prosecuting those who commit violence or other federal crimes in the name of violent domestic ideologies, the Department's approach to the online dimensions of the DVE threat is multi-pronged. For example, the Department notifies online platforms when it identifies terrorism-related online recruitment materials or efforts, so that platforms can enforce their own terms of service that prohibit the use of their platforms for domestic terrorist activities. The Department also works with international partners to share information and coordinate on the transnational linkages, as well as the proliferation of extremist materials via the internet.[xxxix] At the Quintet of Attorneys-General in December 2021, the Attorney General of the United States and the Attorneys-General of Australia, Canada, New Zealand, and the United Kingdom also discussed the challenge of countering the online spread of violent extremist narratives.

As the Department continues to adapt to the increasing DVE caseload, it should continue to find additional ways to combat the internet's role. For example, as recommended in the White House's *National Strategy on Countering Domestic Terrorism*, the Department should continue to enhance the domestic terrorism-related information offered to the private sector, especially the technology sector, and facilitate more robust efforts outside the government to counter terrorists' abuse of Internet-based communications platforms to recruit others to engage in violence.[xl] As the Department increases its understanding of how modern DVE groups operate online through its growing caseload, it should be sure to share what it learns about those TTPs with international and private sector partners.

II. PARTNERSHIPS IN COMBATING CYBER THREATS

An effective and comprehensive cyber strategy requires recognition that neither the Department of Justice nor any other single government agency or private sector firm should combat cyber and cyber-enabled threats alone. Specifically, the Department of Justice should look toward ensuring that it: (1) partners with other members of the U.S. Government to ensure a whole-of-government approach to disrupt cybercriminal activity in a coordinated fashion, for maximum impact; (2) cooperates with international allies and organizations on priority cyber threats, including ransomware, state-sponsored malicious cyber activities, and online child sexual exploitation; (3) facilitates SLTT law enforcement and related efforts to combat cyber threats, particularly those crimes that have been handled by SLTT partners; and (4) works closely with the private sector to apply a whole-of-society approach to cooperatively addressing cyber threats.

The Department of Justice is a key player in combating cyber threats and must continue to work collaboratively with each of its federal, international, SLTT, and private sector partners on this common goal. Each of the Department's key partners brings unique capabilities and tools to the cybercrime fight. Building on lessons learned in the counter-terrorism model, the Department should continue to recognize that, when possible, the impact of law enforcement actions against significant cyber threats can be maximized when taken in tandem with efforts from such partners. Coordination of these cyber efforts ensures that the whole range of available resources may be brought to bear to address cyber threats in a systematic and comprehensive way, for greatest possible consequence.

1. Pairing Department Actions with Other U.S. Government Efforts

The U.S. Government possesses other tools outside of the Department of Justice to combat cyber actors. For example, the Department of the Treasury's Office of Foreign Assets Control (OFAC) can impose sanctions on certain cybercriminals to limit their access to the U.S. financial system and their ability to do business with U.S. persons.[xli] Likewise, the Department of Commerce can restrict the export, re-export, and/or transfer (in-country) of items, including sensitive technologies. The State Department administers several rewards programs that have been used to combat cybercrime, including the Transnational Organized Crime Rewards Program (TOCRP)[xlii] and the Rewards for Justice Program (RFJ).[xliii] Finally, the Department of Homeland Security and Defense Department can issue cybersecurity advisories, concurrently with or independent of the Department's law enforcement investigations and actions, to empower network defenders and thereby disrupt cyber threats.

Both in cases involving national security and criminal cyber threats, the Department has increasingly coupled its investigations and prosecutions with other actions by interagency partners, including the Departments of Homeland Security, State, the Treasury, Commerce, and Defense, as well as the U.S. Intelligence Community (USIC). For example:

- In November 2021, the Department charged two Iranian nationals for their role in a cyber-enabled disinformation and threat campaign designed to influence the 2020

U.S. presidential election.[xliv] Concurrent with the unsealing of the indictment, the Department of the Treasury designated for sanction the two defendants, their employer, and the employer's leadership. Additionally, the State Department's Rewards for Justice (RFJ) Program offered a reward of up to $10 million for information about the defendants' activities.[xlv]

- In March 2020, during the Department's investigation into RGB hackers responsible for hacks of cryptocurrency exchanges around the world (*see* p. 14), the Department executed an interim disruptive action against the RGB's network of criminal launderers.[xlvi] With support of the Defense Department's U.S. Cyber Command, in August 2020, the Department initiated civil forfeiture proceedings against 280 additional cryptocurrency accounts used by the RGB hackers and their Chinese money launderers.[xlvii] Concurrent with the Department's actions, the Department of the Treasury also imposed sanctions on the Chinese nationals and numerous cryptocurrency addresses related to their involvement in activities facilitating North Korea's sanctions evasion.

The Department also regularly works with members of the USIC, in classified settings, to advance the U.S. Government's disruption efforts.

The Department has taken recent steps to deepen coordination with other government agencies, including the assignment of a Department attorney as a liaison to U.S. Cyber Command and the seconding of Department attorneys and FBI employees to the National Security Council's Cyber Directorate as well as the Office of the National Cyber Director. The Department should continue to look for further opportunities to coordinate. In instances where the Department of Justice takes public action aside from the announcement of an arrest of a defendant, such as the unsealing of charges against cybercriminal actors who are located in jurisdictions outside the United States, prosecutors and agents should work toward ensuring that the Department's disruptive actions are aligned with those of its federal partners for maximum impact and consequence. These actions include the potential use of economic sanctions, additions to the Department of Commerce's Entity List, virtual currency regulations, diplomatic pressure, rewards programs, intelligence operations, and military action.

Whole-of-government actions are most effective when different agencies can announce disruption efforts concurrently. For example, a new sanctions program is likely to be more impactful when it is announced close-in-time to the Department's unsealing of an indictment, rather than months or years later. In many cases, concurrent use of different governmental tools has an amplifying effect for disruptive measures.

In order for different governmental tools to be used at the same time, the Department needs to ensure that it is coordinating with other U.S. Governmental agencies at the earliest possible stages, in order to give those agencies time to assess facts and consider what if any actions may be possible, while allowing the other agencies to maintain a timeline for action that syncs to the Department's own anticipated schedule for action. Where appropriate, the Department needs to find ways and have an increased willingness to share information with interagency colleagues, in order for them to have greater visibility into threats and to avoid unnecessary duplication of investigative efforts.

Department Consultation About Intergovernmental Coordination: Prosecutors investigating cyber cases may not have familiarity with the authorities and processes used by other agencies, such as sanctions, export controls, demarches, rewards programs, and the multitude of classified and unclassified tools that can be used to disrupt cyber actors. Likewise, many Department of Justice offices may not have contacts at the U.S. Government offices responsible for these different tools.

For this reason, prosecutors and agents handling sophisticated, transnational cyber threats should, for certain significant cyber investigations that have clear transnational linkages, be required to coordinate with other components of the Department of Justice that have more frequent contact with the interagency process, most notably CRM and NSD. The consultation requirements described above, which could be issued in conjunction with the recommended reporting requirements for transnational cyber and cryptocurrency cases, should instruct investigating offices to consult as to what additional non-prosecutorial tools may be appropriate and available, and provide information about what, if any, other U.S. Government agency is investigating or contemplating actions against the same threat. During their review of reported matters, CRM and NSD should be directed to identify and provide feedback to the prosecuting offices about possible coordinated actions that might be appropriate.

Coordination through the National Cyber Investigative Joint Task Force: An additional path to coordinate interagency action is NCIJTF. The NCIJTF comprises more than 30 partnering agencies from across law enforcement, the intelligence community, and the Department of Defense (DOD), with representatives who are co-located and work jointly to approach the cyber challenge from a whole-of-government perspective. The NCIJTF's primary responsibilities are to coordinate, integrate, and share information to support cyber threat investigations; supply and support intelligence analysis for community decision-makers; and provide value to other ongoing efforts in the fight against the cyber threat to the nation. These efforts support NCIJTF's role under Presidential Policy Directive-41 ("United States Cyber Incident Coordination"), which designates the Department of Justice, through the FBI and NCIJTF, as the lead federal agency for threat response activities in the context of a significant cyber incident.[xlviii]

Because of its multi-agency participation, and its collaboration with international and private sector partners, the NCIJTF is uniquely situated to ensure that the authorities and capabilities of its members can be used to jointly sequence and plan campaigns designed to identify, pursue, and disrupt cybercriminal actors who seek to exploit and attack computer systems. Where appropriate, for priority cyber threats in both the national security and criminal context, the Department should work with the NCIJTF to ensure that a whole-of-government campaign can be developed, including through the use of the Department's investigative holdings, to disrupt the threat through joint, sequenced, and coordinated interagency efforts.

2. International Efforts to Combat Cyber Threats

The transnational nature of many cyber threats—whether criminal, state-sponsored, or a blend of the two—requires that the Department work with international partners to disrupt attacks and hold perpetrators accountable. The Department has developed a significant network of prosecutors, agents, and other personnel dedicated to building partnerships across the globe, both to work with foreign partners on cyber issues and to help other nations build their own capacity to combat these shared cyber threats.

The Department's international efforts cut across its components. The FBI's International Operations Division (IOD) and Legal Attaché (Legat) offices work with foreign law enforcement and intelligence partners to combat threats against the United States, share intelligence, and coordinate FBI investigations with a foreign nexus.[xlix] The U.S. Transnational and High-Tech Crime Global Law Enforcement Network (GLEN), operated by the Criminal Division in partnership with the State Department, is a worldwide law enforcement capacity-building network of attorneys, forensic analysts, and law enforcement agents who deliver training and technical assistance to foreign partners.[l] CRM's Office of International Affairs (OIA) and CCIPS, as well as NSD's Law and Policy Office (L&P), all participate through multiple international forums to work with foreign partners on cyber issues. CRM's MLARS also works with international partners to set global standards to combat money laundering, terrorist financing, and other related threats to the integrity of the financial system.

> *"[J]ust like the alliances we formed to fight the battles of the past, our efforts are so much more powerful when combined with those of our international partners. Evolving to match the cyber threat does not only mean new tools and teams within the Department of Justice – it means finding innovative ways to work with our international partners."*
>
> DAG Lisa O. Monaco, DAG Lisa O. Monaco, Address at Annual Munich Cybersecurity Conference (Apr. 20, 2022)

In recent years, the Department executed several successful operations with international partners to disrupt cyber-enabled threats, including actions taken against the Emotet botnet (*see* p. 28) and the disruptive actions taken against the Sodinokibi/REvil ransomware group (*see* p. 35). The commitment of international partners and the Department's engagement with these partners are critical to the Department's success, as those who conduct ransomware, hacking, and other cyberattacks target victims across the world without respect for borders. In this same vein, the Department has established the International Virtual Currency Initiative (*see* p. 30), focused on strengthening international law enforcement efforts to combat the illicit use of digital assets. Given the proliferation of threats, the Department should welcome new opportunities to work with international partners to interdict cyber and cryptocurrency threats.

Emotet Botnet Disruption

In January 2021, the Department of Justice participated in a multinational operation with Canada, France, Germany, the Netherlands, the United Kingdom, Lithuania, Sweden, and Ukraine to disrupt and take down the infrastructure of the malware and botnet known as Emotet. This technical disruption, which was coordinated across multiple international jurisdictions, is a key public example of efforts that the Department of Justice has undertaken to use all of its available authorities to combat cybercrime in conjunction with its public and private partners around the world.

Emotet is a family of malware that targets critical industries worldwide, including banking, e-commerce, healthcare, academia, government, and technology. It caused hundreds of millions of dollars in damage worldwide. Emotet malware primarily infects victim computers through spam email messages containing malicious attachments or hyperlinks. Once it has infected a victim computer, Emotet can deliver additional malware to the infected computer, such as ransomware or malware that steals financial credentials. Computers infected with Emotet malware became part of a botnet (*i.e.*, a network of compromised computers) that malicious cyber actors can remotely control in a coordinated fashion, while owners and operators of the victim computers are typically unaware of the infection.

Foreign law enforcement agents, working in coordination with the FBI, gained lawful access to Emotet servers located overseas and identified the IP addresses of approximately 1.6 million computers worldwide that appeared to have been infected with Emotet malware between April 1, 2020, and January 17, 2021. Of those, over 45,000 infected computers appeared to have been located in the United States.

Foreign law enforcement, working in collaboration with the FBI, replaced Emotet malware on servers located in their jurisdiction with a file created by law enforcement, according to the affidavit. This was done with the intent that computers in the United States and elsewhere that were infected by the Emotet malware would download the law enforcement file during an already-programmed Emotet update. The law enforcement file prevented the administrators of the Emotet botnet from further communicating with infected computers. The law enforcement file did not remediate other malware that was already installed on the infected computer through Emotet; instead, it was designed to prevent additional malware from being installed on the infected computer by untethering the victim computer from the botnet. The scope of the Emotet law enforcement action was limited to the information installed on infected computers by the Emotet operators and did not extend to the information of the owners and users of the computers.

The FBI, in coordination with foreign law enforcement officials, also gained lawful access to an Emotet distribution server located overseas and identified several servers worldwide that were used to distribute the Emotet malware. These servers were typically compromised web servers belonging to what appeared to be unknowing third parties. The perpetrators uploaded the Emotet malware to the servers through unauthorized software applications. Victims who clicked on spam email messages containing malicious attachments or hyperlinks would then download the initial Emotet malware file from a distribution server. The FBI also notified more than 20 U.S.-based hosting providers that they hosted more than 45 IP addresses that had been compromised by the perpetrators associated with the Emotet malware and botnet. FBI Legal Attachés further notified authorities in more than 50 countries that hosting providers in their respective jurisdictions hosted hundreds of IP addresses that were compromised by Emotet.

International Virtual Currency Initiative

Since the earliest inception of digital assets, the Department of Justice has led the way in combating their misuse in furtherance of criminal activities, from the prosecution of the digital currency exchange E-Gold even before the advent of cryptocurrency, to the takedown of Silk Road, the first darknet market for which all transactions were conducted in bitcoin. The illicit use of digital assets has now grown to intersect with many of the Department's investigations. This includes the use of digital assets to facilitate ransomware payments in the wake of attacks conducted by criminal and nation-state cybercriminals alike; narcotics trafficking; the sale of child sexual exploitation materials; terrorism and sanctions evasion; and money laundering. But because these crimes—and the virtual currency financial infrastructure itself—cross international borders, efforts to combat the criminal abuse of digital assets necessarily require an international approach. To ensure success in its efforts to investigate cases involving digital assets, the Department must work closely with and rely upon its foreign law enforcement and regulatory partners.

In furtherance of this mission, the Department has established the **International Virtual Currency Initiative**, focused on strengthening international law enforcement efforts to combat the illicit use of digital assets. This Initiative will seek to build capacity in our foreign law enforcement partners, strengthen relationships with those partners to better collaborate on investigations and prosecutions, support efforts both within the United States and abroad to assure that virtual currency exchanges and other financial entities comply with reasonable regulatory rules such as the anti-money laundering requirements developed by the Financial Action Task Force (FATF), and work to identify and recommend additional measures that may be taken to tackle the international dimensions of the illicit use of digital assets.

First, the Criminal Division, through the Global Law Enforcement Network (GLEN) of International Computer Hacking and Intellectual Property (ICHIP) Attorney Advisors, operated in partnership with the Bureau of International Narcotics and Law Enforcement Affairs of the Department of State, will work to strengthen international cooperation and capacity with respect to the illicit use of cryptocurrency. Building on existing efforts and plans, regional ICHIP advisors, led by the ICHIP focused specifically on cryptocurrency and the dark web and supported by the National Cryptocurrency Enforcement Team (NCET), will run three regional Cryptocurrency Working Groups in Southeast Asia, Eastern Europe, and Latin America. These Working Groups will deliver sustained, case-based mentoring and training, exchange of best practices, and identification of enforcement gaps and trends in illicit use of cryptocurrency in partnership with other countries in those regions. They will seek to build relationships of trust and cooperation among working group members, foster work with Department prosecutors and U.S. law enforcement agencies, and create opportunities for the ICHIPs to conduct additional specific, country-focused assistance to judges, prosecutors, investigators, and forensic analysts. Building foreign capacity to combat criminal activity involving cryptocurrency in this fashion will develop reliable and capable foreign counterparts and the interoperability necessary for the Department's operational success.

Second, Resident Legal Advisors (RLAs) funded by the State Department's Counterterrorism Bureau will increase their focus on the use of virtual currencies to fund terrorist organizations. Terrorism financing, which is the basis of terrorist activities and the lifeblood of terrorist organizations, has unfortunately found a safe harbor through the increased use of cryptocurrency. Consequently, these counter-terrorism focused RLAs will step up the integration of cryptocurrency awareness and training into their capacity-building programs.

Third, the Department will work closely with the Department of the Treasury, the Department of State, and our international partners to pursue the implementation of global anti-money laundering and counter financing-of-terrorism (AML/CFT) standards for virtual assets and virtual asset service providers (VASPs). Evolving regulatory regimes have produced inconsistencies and gaps in regulation and supervision of virtual assets and VASPs in some regions of the world. These fractured AML/CFT regulatory regimes jeopardize the safety and stability of the international financial system and create opportunities for criminal actors to take advantage of the regulatory inconsistencies. The Department, as part of the Department of the Treasury-led U.S. delegation to the FATF, will pursue international efforts to seek implementation of the FATF standards. The Department will also continue to work with the Department of the Treasury and others to implement a range of new AML/CFT authorities enacted by Congress in early 2021, which include new requirements for the collection and reporting of information on the beneficial owners of certain corporate structures, as well as the expansion of key definitions in the Bank Secrecy Act to include certain activities involving virtual assets.

Finally, the NCET will work to identify and recommend additional measures that can be taken to strengthen international law enforcement cooperation to address and combat criminal activity related to digital assets. In doing so, the NCET will coordinate with components across the Department, building on the lessons learned across these lines of effort and the Department's experience in investigating misuse of digital assets here and abroad, as well as with the Department's key domestic partners, including the Departments of State, the Treasury, and Homeland Security.

Extraditions and Expulsions: CRM's OIA is responsible for coordinating extradition and expulsion requests. Recently, the Department has had multiple notable extradition achievements for alleged cyber criminals. For example, in October 2021, South Korea agreed to extradite a Russian national to the United States based on charges alleging his involvement in deploying the Trickbot malware.[li] In November 2021, the Department achieved its first-ever conviction of a foreign intelligence officer responsible for cyber intrusions against the United States, after the first-ever extradition of a foreign intelligence officer from Belgium.[lii] Finally, in December 2021, Switzerland extradited a Russian national to the United States based on federal charges related to alleged hacking into computer systems in order to gain material non-public information that was then used to commit insider trading.[liii] These successes are not unique; since 2018, the Department has extradited alleged cybercriminals from at least twenty-two different countries (*see* p. 33).

The Department should continue to seek extradition or expulsion whenever possible and plan for such requests as early as possible. To that end, encouraging prosecutors to consult with OIA on significant cyber investigations with transnational linkages will help ensure that prosecutors are preparing requests appropriately early, given the significant time that can be needed to prepare and transmit the requests.

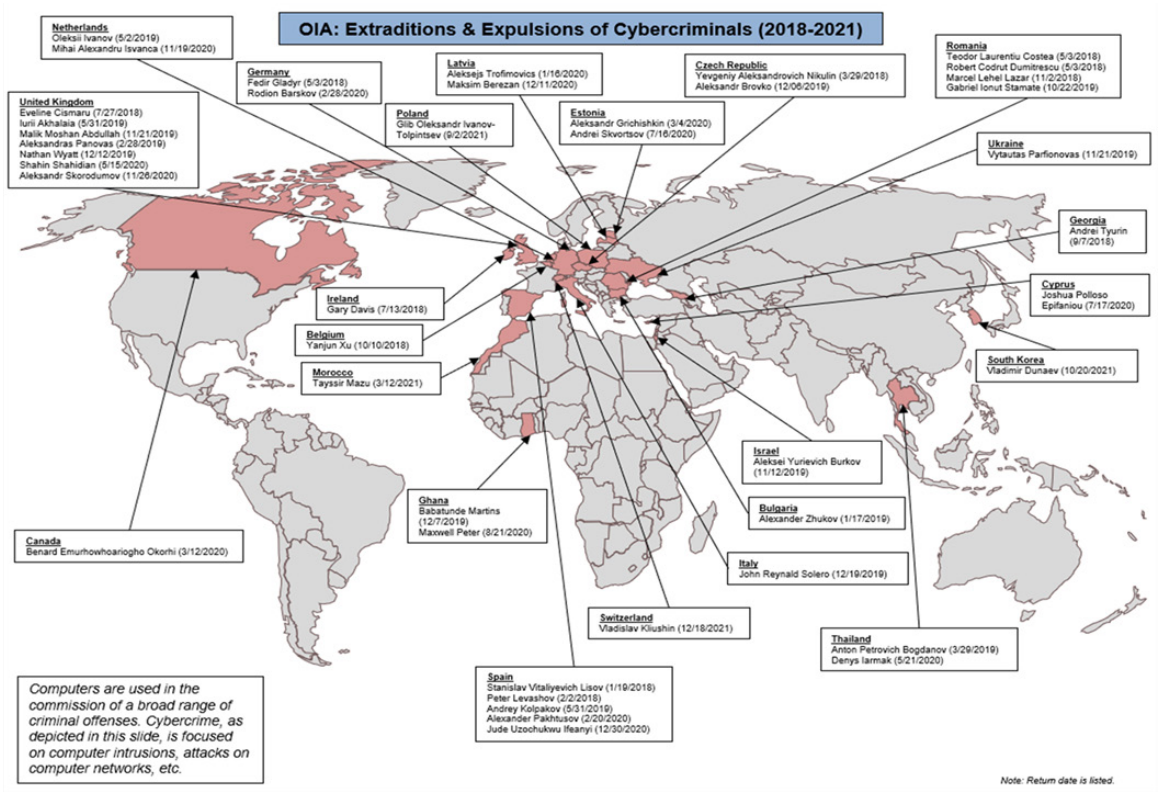

Figure 2 – Extraditions and Expulsions of Cybercriminals from 2018 to 2021

Coordinated International Responses: In recent years, the Department's investigations have provided the foundation for coordinated international responses to malicious cyber activities, allowing for the rebuttal of an accused nation state's denials, enhancement of diplomatic efforts to galvanize international opinion against malicious cyber activities, the establishment of bilateral relationships around cyber issues, and/or the strengthening of international network defense activities, and coordinated public and non-public disruption actions.

The deterrent effect of Department actions is amplified when coupled with parallel actions from its international partners, such as those in the Sodinokibi/REvil arrests (*see* p. 35). But, even if parallel disruptive actions by the United States and its international partners are not conducted at the same time or in a manner visible to the public, they still reinforce each other and together help establish norms of responsible state behavior in cyberspace.[liv]

Prosecutors, therefore, should look proactively for opportunities to work with overseas Department prosecutors, the FBI's cyber-focused Assistant Legal Attachés (ALATs) stationed at embassies around the world, and international partners, recognizing that a "go at it alone" mentality may sometimes sacrifice effectiveness in the name of expediency. While unilateral action will sometimes be necessary, prosecutors and case agents should regularly consult with counterparts in the Department—most notably with CCIPS, OIA, NSD's Counterintelligence and Export Control Section (CES), Legats, and FBI IOD—about what possible international

responses could be available, and what would facilitate those international responses. To that end, as part of the recommended new reporting and consultation guidance on cyber and cryptocurrency investigations (*see* p. 8), prosecutors should be required to identify what if any international coordination or parallel actions are being contemplated to disrupt the cyber threat. Where appropriate, CCIPS, OIA, and CES shall recommend additional international engagement to the prosecutors.

Another way to increase international coordinated operations is the designation of a prosecutor to focus on looking for and seizing such opportunities. To that end, the Department will designate a prosecutor with significant experience in coordinating international disruptions to a new position as a **Cyber Operations International Liaison (COIL)**. The COIL will focus on top-tier actors in the cybercrime ecosystem, as identified by, and in coordination with, other Department components and government partners, and increase the tempo of international coordinated disruptions against these actors. Such disruptions should include criminal charges and arrests, asset seizures, dismantlement of infrastructure, public attribution statements, cybersecurity advisories, and the deployment of the EU's Cyber Diplomacy Toolkit (and similar non-law enforcement measures).

The COIL will have a two-way responsibility, both in identifying opportunities to couple international partners' actions to the Department's ongoing investigations, and in increasing U.S. prosecutorial and law enforcement awareness about ongoing high-profile cyber investigations being conducted by foreign partners. To carry out that responsibility, the Department, including the FBI and OIA, should ensure that the COIL has: (i) visibility into cyber-related information exchanges with foreign counterparts (*e.g.*, meetings, "foreign disseminations," and mutual legal assistance (MLA) requests); and (ii) the necessary investigative file accesses to allow the COIL to identify and assess opportunities for collaboration between U.S. law enforcement and foreign partners. The COIL should also work with the GLEN, CCIPS, OIA, the Office of Overseas Prosecutorial Development (OPDAT), and CES to identify, train, and connect competent cybercrime prosecutors and investigators in partner countries who can be enlisted in an international effort to impose costs on elite cybercriminals, state-sponsored cyber actors, and facilitators, wherever they are located.

The COIL will likely be most effective when operating out of Europe, where the majority of international coordinated efforts on cybercrime and cyber-based threats have occurred. Within the first year of the COIL program, the Department will evaluate whether at least one prosecutor in a COIL role should be deployed overseas, such as to a major European capital, to continue this work against elite cyber threats.

> *"So you see that we are deploying forward to meet this threat, and looking to build on our past successes in order to have a more lasting impact on the ransomware menace."*
>
> DAG Lisa O. Monaco, Address at Institute for Security and Technology (May 15, 2022)

Actions against the Sodinokibi/REvil Ransomware Group

In November 2021, the Department announced coordinated actions against two individuals suspected of deploying Sodinokibi, also known as REvil, ransomware against U.S. and other victims, including the arrest of Ukrainian national Yaroslav Vasinskyi by the Polish police at the request of U.S. officials and the seizure of $6.1 million in cryptocurrency traceable to REvil ransomware attacks by Russian national Yevgeniy Polyanin. The Department of Justice's actions were announced as part of a whole-of-government disruption effort against Sodinokibi/REvil, which included the announcement by the Department of the Treasury's OFAC, designating Vasinskyi, Polyanin, and entities related to Chatex, a virtual currency exchange that facilitated financial transactions for ransomware actors; as well as the Department of State's announcement of a reward of up to $10,000,000, under its Transnational Organized Crime Rewards Program, for information leading to the identification or location of any individual holding a key leadership position in the Sodinokibi/REvil group.[lv]

Figure 3 –Attorney General Merrick B. Garland at Sodinokibi/REvil Press Conference, November 8, 2021

Both Vasinskyi and Polyanin were charged with accessing the internal computer networks of several victim companies and deploying Sodinokibi/REvil ransomware to encrypt the data on the networks of victim companies. In addition, court documents alleged that Vasinskyi was responsible for the July 2021 attack against Kaseya, a multinational information technology company. In the attack against Kaseya, Vasinskyi is alleged to have caused the deployment of malicious Sodinokibi/REvil code throughout a Kaseya product that caused the Kaseya production functionality to deploy REvil ransomware to "endpoints" on Kaseya customer networks. After the remote access to Kaseya endpoints was established, the ransomware was executed on those computers, which resulted in the encryption of data on computers of organizations around the world that used Kaseya software.

Through the deployment of Sodinokibi/REvil ransomware, the defendants allegedly left electronic notes in the form of a text file on the victims' computers. The notes included a web address leading to the TOR network, as well as the link to a publicly accessible website address the victims could visit to recover their files. Upon visiting either website, victims were issued a ransom demand and provided a virtual currency address to use to pay the ransom. If a victim paid the ransom amount, the defendants provided the decryption key, and the victims then were able to access their files. If a victim did not pay the ransom, the defendants typically posted the victims' stolen data or claimed they had sold the stolen data to third parties, and victims were unable to access their files.

Vasinskyi was taken into custody in Poland, and in March 2022 was extradited to the United States pursuant to the extradition treaty between the United States and the Republic of Poland. In parallel with the arrest, interviews and searches were carried out in multiple countries, and would not have been possible without the rapid response of the National Police of Ukraine and the Prosecutor General's Office of Ukraine. The Department of Justice's actions were coordinated with those taken by Europol countries, including the arrest of five additional individuals suspected of deploying the Sodinokibi/REvil ransomware, as part of its joint international law enforcement effort involving Australia, Belgium, Canada, France, Germany, the Netherlands, Luxembourg, Norway, Philippines, Poland, Romania, South Korea, Sweden, Switzerland, Kuwait, and the United Kingdom.[lvi]

Access to Electronic Evidence Abroad: Access to electronic evidence is critical to successfully combat cybercrime. One significant way to increase the collective security of the United States and its allies is to ensure reciprocal access to digital evidence in foreign jurisdictions. The Department continues to work to improve law enforcement and prosecutor access to electronic evidence stored abroad. For example, the Department recently concluded negotiations of a Second Additional Protocol to the Budapest Convention on Cybercrime, which is specifically designed to help law enforcement authorities obtain access to electronic evidence held in other countries.[lvii]

OIA plays a key role in both obtaining electronic evidence from foreign partners to assist domestic investigations and helping foreign partners to obtain electronic evidence from the United States. Given the ever-increasing number of requests for electronic evidence from U.S. service providers, OIA created a Cyber Team focused on reviewing and executing requests for electronic evidence received from foreign partners. The Cyber Team further provides training to foreign authorities to better facilitate successful MLA requests to the United States.

A significant line of effort for the Department is the negotiation of executive agreements pursuant to the CLOUD Act, which permits the United States to enter into bilateral executive agreements between the United States and foreign countries for the direct sharing of electronic evidence, without needing to use the MLA request process. Traditionally, evidence in foreign jurisdictions has been obtained through mutual legal assistance treaties (MLATs). The MLAT process, however, is overwhelmed with requests as evidence increasingly exists overseas for even the most domestic of crimes. Due to the volume of foreign government requests seeking electronic evidence in the custody or control of U.S.-based service providers, and the pressure those requests were placing on the smooth functioning of the MLAT process, in 2018 Congress passed the CLOUD Act.[lviii]

Since passage of the CLOUD Act, the Department has completed CLOUD Act agreements with two countries. In October 2019, the United States and United Kingdom signed the first-ever agreement pursuant to the CLOUD Act; however, that agreement has not yet entered into force. In June 2021, President Biden and Prime Minister Boris Johnston committed to bringing the CLOUD Act agreement into force based on a mutual recognition that both countries have an appropriately high level of data protection, noting that doing so would "allow[] law enforcement investigations on both sides of the Atlantic to obtain the evidence needed to bring offenders to justice, whilst maintaining rigorous privacy standards."[lix] The Department continues to work toward that goal with its U.K. counterparts.

Separately, on December 15, 2021, Attorney General Garland signed a CLOUD Act agreement on behalf of the United States with Australia. The CLOUD Act agreement will help ensure Australian and U.S. law enforcement agencies are able to timely access electronic data to prevent, detect, investigate and prosecute serious crime, including ransomware attacks, terrorism and the sabotage of critical infrastructure over the internet, and child sexual abuse. The U.S.-Australian CLOUD Act agreement is expected to enter into force later in 2022.

Figure 4 – Australian Minister for Home Affairs Karen Andrews and Attorney General Merrick B. Garland at Signing of CLOUD Act Agreement, December 15, 2021

The Department continues to negotiate possible CLOUD Act agreements with its partners, and it should continue to make such negotiations a priority based on the increasing need for such evidence.

3. State, Local, Tribal, and Territorial Investigative Partnerships

Many types of cyber investigations are investigated principally by SLTT jurisdictions, including online child sexual exploitation (*see* p. 22) and technology-facilitated violence and abuse (*see* p. 21). These agencies in turn face challenges in keeping pace with the ever-changing nature of cyber threats and acquiring the necessary technical expertise, experience, and capabilities needed for successful investigations and prosecutions. The Department of Justice plays a key role in the development and delivery of specialized cybercrime training and technical assistance to SLTT law enforcement partners, led by the OJP.

Building SLTT Investigative Capacity: The OJP's BJA funds two nationwide programs to enhance SLTT law enforcement cyber capacity through training and technical assistance—the Law Enforcement Cyber Center (LECC) and the National White-Collar Crime Center (NW3C). The LECC operates as a national clearinghouse of information and resources for law enforcement and justice agencies to prevent, investigate, prosecute, and respond to cyber threats and related crimes. LECC information is curated, vetted, and easily accessible to help investigators and prosecutors understand the cyber environment, identify emerging trends, leverage promising practices, and promote innovative solutions and collaboration.

With over 110,000 active users, NW3C delivers specialized, no-cost training and technical assistance in the areas of, among other things, digital forensics, criminal intelligence, and responses to cyber threats. Emerging and specialized topics (ransomware, cyberstalking, deep fakes, internet of things, social media networking, etc.) are addressed via supplemental

training and national practitioner webinars. In addition to training, NW3C provides various forms of technical assistance to SLTT law enforcement partners, including guidance on best practices, policies, information technology (IT) security, personnel development, and overall readiness to respond to cyber threats and related crimes. NW3C also provides direct assistance to support investigations in the form of subject matter expertise to assist with specific cyber challenges.

Separately, the OJP Office of Juvenile Justice and Delinquency Prevention (OJJDP) established the Internet Crimes Against Children (ICAC) Task Force Program, to assist state, local and tribal law enforcement agencies in developing an effective response to technology-facilitated child sexual exploitation and Internet crimes against children. The ICAC program is a national network of 61 coordinated task forces representing more than 5,400 federal, state, local and tribal law enforcement and prosecutorial agencies. These agencies are engaged in both proactive and reactive investigations, digital forensic investigations, and criminal prosecutions. In Fiscal Year (FY) 2020, the ICAC task forces conducted more than 109,000 investigations resulting in the arrest of more than 9,200 individuals.

Cybersecurity of SLTT Partners: The Department of Justice has important partnerships with SLTT law enforcement partners. Many of these partners operate their own computer systems that retain important and sensitive data about ongoing operations, identities of human sources, and so on. SLTT law enforcement systems also have access to federal law enforcement data, whether through access to joint databases or through operations in which SLTT agencies participate as partners in federal task forces and other law enforcement operations.

For these reasons, SLTT partner-operated systems are often the targets of the same types of cybercriminals that constantly target the Department's own systems. In order to protect Department of Justice data and operations from malicious actors, the Department must also be ready to assist SLTT law enforcement agencies with protecting their own systems—through technical assistance, information-sharing about ongoing threats, and appropriate cybersecurity standards for jointly accessed systems.

For instance, to facilitate law enforcement collaboration and partnership, the Department also has helped establish multiple online platforms through which SLTT partners can access tools and resources for all kinds of law enforcement subjects, including the Law Enforcement Enterprise Portal (LEEP)—a secure platform for law enforcement agencies, intelligence groups, and criminal justice entities that provide web-based investigative tools and analytical resources to facilitate law enforcement collaboration and partnership. Giving partners access comes with attendant cybersecurity risks, as a compromised partner's system could become a way to access the data on these platforms. The Department therefore needs to monitor these platforms for signs of compromise in the same way the Department monitors its own systems. The same requirements imposed to access Department systems—multifactor authentication, identity management systems, periodic auditing managed by the Department, and so on—should be required for these systems.

In addition, the Department already provides funding and additional support to some SLTT groups so that they can maintain identity management systems to access LEEP as well as other portals. The Department should continue to provide significant support to SLTT partners to ensure they maintain resilient systems and look for additional opportunities to enhance the security for the systems that it helps fund.

4. The Private Sector

Recent major cyber incidents have made plain that cooperation between the Department of Justice and the private sector is vital to meeting the cyber challenge. In the words of the FBI Director, successfully combating threats requires an "enterprise approach—one that involves government agencies, private industries, researchers, and non-profits across the U.S. and the world." The collective model of action, in which the Department of Justice and its government partners work in strong partnership with the private sector, is crucial to common security, by providing a comprehensive picture of cyber threats and incidents, and a path toward hardening collective defenses.

A. The Need for Private Sector Assistance

The private sector operates as an early warning system to cyber threats, a partner in remediation, and a collaborator in new defense strategies. The Department participates in a number of collaborations with the private sector—some through more institutionalized paths of collaboration, and others through informal avenues of cooperation. For example, through the National Center for Missing and Exploiting Children (NCMEC), law enforcement received more than 21.4 million tips from electronic service providers in 2020 about possible online child sexual exploitation.[lxi] Preserving and strengthening these pathways for informational exchange helps support a more forewarned, and therefore more secure, environment for the private sector and public alike.

Like the Department of Justice and others in government, many in the private sector are targets and victims of sophisticated cyber threats, whether those breaches are motivated by espionage, illicit profit, or state-sponsored geopolitical interest. When private sector entities or persons are the victims of cyber incidents, it is imperative that they come forward to provide investigators with enough information to investigate and disrupt the threat. Information provided by private sector victims and technology companies attempting to protect their users is crucial to disruption efforts, allowing the Department of Justice to identify additional evidence, victims, and criminal infrastructure used by malicious cyber actors. Information gained by the Department over the course of its investigations is shared with law enforcement and intelligence partners, as appropriate, to further their efforts, which in turn leads to a more comprehensive threat profile. Certain information gained over the course of the investigation is also shared, in many cases with its source anonymized, with the private sector to strengthen their own defenses against the threat, and to better protect the nation's economic, national, and personal security from further attacks.

> *"The bottom line is this: I believe it is bad for companies, bad for America, and it hurts our efforts to uphold the values that we try to demonstrate as a country, if companies are attacked and don't partner with law enforcement, and thereby help disrupt these activities and prevent future victims."*
>
> DAG Lisa O. Monaco, Address at Criminal Division Cybersecurity Roundtable: The Evolving Cyber Threat Landscape (Oct. 20, 2021)

The Department recognizes victims are sometimes hesitant to report cybercrimes for a variety of reasons. To mitigate such hesitancy, therefore, the Department must make reporting as easy as possible in order to avoid bureaucratic red tape adding to a victim's recalcitrance to

come forward. Even marginal improvements in "victim engagement" can have significant effects on the number of crimes reported to the Department.

As the array of government departments and agencies involved in cyber incidents broadens, the Department recognizes that government outreach to the private sector needs to be streamlined where appropriate to avoid a cacophony of duplicative or conflicting government voices. The Department has looked to increase its coordination with other government departments and agencies—most notably CISA and the Intelligence Community—to sync messaging and engagement with the private sector, and it should continue to do so.

The Department should always look to work collaboratively with the private sector in preventing, disrupting, and mitigating cyber incidents and attacks. However, the Department should also ensure that companies comply with any existing legal obligations to provide information and produce evidence that is relevant to ongoing investigations. If companies routinely fail to fulfill such obligations, the Department has and should continue to consider all legal recourse, including seeking contempt orders and financial penalties for failure to comply with court orders. Likewise, the Department should also carefully evaluate instances where companies fail to report incidents to regulators, in violation of statutory or regulatory obligations.

B. Supporting Private Sector Cybersecurity Efforts

The Department has long worked with private industry to improve collective cybersecurity. Since 2015, for example, CCIPS's Cybersecurity Unit has conducted outreach and issued guidance on cybersecurity issues to frequently targeted sectors of the U.S. economy, including critical infrastructure and cyber incident response firms, as well as interagency partners.[lxii] Likewise, the FBI's Office of Private Sector provides a connection between industry leaders and FBI professionals to discuss emerging threats to the private sector, including cyber intrusions, cyber-enabled espionage, and ransomware. Each of FBI's 56 field offices has a Private Sector Coordinator, who serves as the primary liaison with members of the private sector.

Another way the Department assists private sector efforts is through information-sharing about ongoing threats. The FBI disseminates information regarding specific threats to the private sector through various methods, including Private Industry Notifications (PINs) and FLASH reports, in order to provide unclassified information that will enhance the private sector's awareness of a threat. These communication methods facilitate the sharing of information with either a broad audience or a specific sector. The FBI also works with industry partners in forums such as InfraGard and industry-based Information Sharing and Analysis Centers to relay critical information.[lxiii]

In the course of the review, many in the private sector and other government agencies noted the need to be conscious of coordinating the alerts and other information about cyber incidents that are relayed to the field. Given the multiple government agencies bearing some responsibility for engaging the private sector, uncoordinated updates run the risk of being duplicative or, in some cases, contradictory. To that end, the Department has concertedly worked with other agencies (most notably CISA and the National Security Agency (NSA)) to increase the number of jointly published updates on ongoing threats. Over the last year, so-called "tri-seal" advisories on cybersecurity threats—jointly issued by the FBI, CISA, and NSA—have increasingly become the norm.[lxiv] The FBI should continue this trend, including working on ways to increase the ease with which joint advisories can be issued.

C. FBI Victim Reporting Systems

The FBI receives hundreds of thousands of complaints a year from people who believe they have been the victim of cybercrime. The FBI's National Threat Operations Center fields approximately 3,100 phone calls and electronic tips from the public at its facility in Clarksburg, West Virginia. The principal means for reporting internet crimes to the Department is the FBI's Internet Crime Complaint Center (IC3). Established in 2000, IC3 originally focused on the emerging trend of internet fraud. In calendar year 2021, IC3 received a total of 959,584 complaints with total losses over $21 billion.[lxv]

The IC3 also serves as the primary intake facility for the execution of both the IC3 Domestic Recovery Asset Team (RAT) and International Financial Fraud Kill Chain (FFKC).[lxvii] The RAT is an IC3 initiative to assist in the identification and freezing of fraudulent funds related to business email compromise incidents. Since inception, February 2018, through December 2021, the RAT team addressed 5,348 incidents that reached the thresholds for potential domestic freezing of funds, reporting losses of $1.5 billion. RAT froze and made available for recovery over $1.2 billion, an overall success rate of 78%.

IC3 has also partnered with other parts of the Department to increase victim engagement on particular areas of Internet-based fraud. For example, in recent years, IC3 has worked with the Elder Justice Initiative to increase reporting of online fraud targeting the elderly, including the publication of the 2020 Elder Fraud Report that provides information useful for targeting interventions.[lxviii] Likewise, in 2021, IC3 took steps to increase reporting on ransomware as part of the Department's collective efforts to combat the emerging trend.

While IC3 will continue to be a vital way for victims to report cybercrime to the Department, there are several ways in which the Department can improve the victim experience of reporting crimes. First, the Department can improve the visibility of victim-reporting systems through a greater online presence, such as individuated websites dedicated to the specific types of fraud being reported or using more colloquial branding (*e.g.*, "StopFraud.gov" rather than the "Internet Crime Complaint Center"). This type of engagement would decrease victim confusion and help direct them to additional information.

Victims have varying levels of familiarity with technical specifications that can provide the most important evidence for cyber investigators. Asking overly technical questions can frustrate victims and deter reporting. Simplified questions that can account for the type of crime and victims' technical knowledge may increase response rates. Due to historical resource limitations, IC3 currently follows a largely standard intake form for all reporting of internet crime. IC3 should instead develop reporting mechanisms that dynamically respond to victim responses, with a goal of decreasing victim frustration and increasing reporting.

The data collected by IC3 is one of the most fruitful ways for the Department to identify trends and other important linkages between criminal incidents. To complete a thorough analysis, identify patterns, and properly visualize volumes of collected data, the Department needs sophisticated tools and software applications, including robust database management software, statistical software, and geographic information software. As part of its review process, FBI should review its current capabilities and invest in appropriate analytical tools.

D. Incentivizing Earlier Reporting of Crimes Identified by Technology Firms

Because cybercriminals use infrastructure and other online services offered by U.S. technology companies in furtherance of their criminal activity, such companies are increasingly devoting human and technological resources towards identifying the misuse of their platforms and protecting their customers. Although in some cases these companies lawfully report these crimes to law enforcement, unfortunately, too often these companies do not proactively report observed crimes to law enforcement, or rely on *ad hoc* relationships to do so at a time of the companies' choosing. In many cases over the last decade, these companies have proactively taken independent actions against cybercriminals (and other criminals abusing their services) without prior coordination with law enforcement (*e.g.*, law enforcement receives notification only 24 hours in advance, after-the-fact notification, or none at all). Too often this results in lost opportunities for long-term disruption of cybercriminals using tools uniquely available to the U.S. Government.

The Department supports U.S. technology companies' efforts to protect customers. However, there is no reason that criminal activities in the cyber context should be handled differently than in the real world, where it would almost be unheard of for private companies to observe criminal activity either on their premises, or targeting the U.S. public or U.S. interests, without proactively informing U.S. law enforcement at the earliest opportunity and then working with law enforcement to further identify and disrupt such activity. Accordingly, the Department should work with the top U.S. technology companies to develop a voluntary set of principles regarding the proactive and systematic reporting of cybercriminal activities using their platforms (a digital version of "If You See Something, Say Something") with an eye towards protecting communities and collective interests through cooperative disruption.

E. Holding Technology Firms Accountable for Violations of Legal Obligations

Criminal actors, including cybercriminals, use a variety of online services offered by U.S. technology companies, including communication and storage accounts. This evidence oftentimes serves as the lynchpin to a successful investigation and disruption by identifying the existence of a crime, the individuals responsible for the crime, their location, their other hacking infrastructure, and the proceeds of their acts. As easy as it is for criminal actors to set up online accounts to use in their crimes, they can also easily delete and destroy this crucial evidence to hide their tracks from law enforcement.

In certain instances, technology companies fail to comply with their obligations under the law to search their data repositories, preserve evidence, and to respond to subpoenas, court orders, or search warrants in a timely fashion. Federal law requires companies to preserve information within their custody and control upon service of a preservation request, and to produce information when the Government serves upon them valid legal process. Yet sometimes, providers will take weeks, if not months, to return the data. In other cases, companies will produce no data in response to process because they failed to preserve the relevant account. By comparison, if the U.S. Government obtains a warrant to search a location, agents must execute that search within days of the magistrate judge signing the warrant. In addition, there have been instances of highly sensitive investigations that have been compromised due to a provider's failure to abide by a court order not to notify subjects or targets of an investigation about the process that has been served upon the provider.

The failure of certain technology companies to meet their legal obligations significantly hinders investigations in a wide range of cases, from hacking to online child sexual exploitation to violent crimes; this failure is a major factor in allowing criminals to escape detection and apprehension. In many cases, the cause of this problem is that providers consider complying with legal process obligations, and the resulting benefits to protecting public safety from effective law enforcement, as secondary to other business considerations, and in certain instances choose not to prioritize responses to valid and court-issued legal process. For example, some companies refuse to hire enough staff to respond to legal process or equip their staff with outdated and slow data query tools. In some cases, when law enforcement alerts a company to its ability to access and search certain data, companies "engineer away" (*i.e.*, eliminate) such capabilities. Similarly, some providers equip their service and threat intelligence personnel with advanced tools and access to data that is not also made available to personnel responding to legal process. In some cases, providers have not only deliberately refused to produce data that they have in their possession but have also created processes to ensure that they cannot produce information to the Government absent alerting subjects and targets of the investigation that the requests have been made.

Although the Government has repeatedly attempted to work with providers on resolving these issues in a variety of different investigations, it is apparent that more needs to be done to hold providers to account when they choose not to comply with valid legal process. Prosecutors and agents should attempt to resolve any failures by technology companies by engaging with them directly and advising CRM and NSD before or immediately after such engagements to ensure Department-wide visibility and coordination. However, in instances where prosecutors and agents do not receive data in a timely fashion, or a company has otherwise failed to abide by its legal obligations, prosecutors and agents should take additional steps to enforce compliance, including bringing provider personnel before the grand jury, pursuing relief with the court in the form of motions to compel, and seeking sanctions where necessary.

III. RESILIENCE AGAINST CYBER INCIDENTS AND ATTACKS

In December 2020, the Department of Justice identified a serious breach of its Microsoft O365 email environment. That breach ultimately traced back to the compromise of SolarWinds's Orion software and the actors' subsequent leveraging of unrelated failures in O365 security features to expand their access from one compromised component to the Department's broader O365 environment (collectively, the "2020 Breach"). This incident underscored that the Department of Justice will continuously be targeted by the world's most sophisticated malicious cyber actors, due to the important criminal, national security, and other work it performs. The incident also made clear that a successful breach of the Department's networks will threaten to undermine its ability to carry out its mission, as well as risk exposing information that jeopardizes economic, national, and personal security.

The Department has spent the year since the incident identifying ways to reduce both the likelihood of another successful intrusion, and the damage resulting from such an intrusion. The review has evaluated topics including network architecture, data transmission practices, mobile security, and response protocols to cyber incidents. The review also considered ways to ensure that the Department's contractors and vendors follow and maintain appropriate levels of cybersecurity.

The Department does not face the challenge of stopping sophisticated cyber operations on its own. The White House has been active in addressing today's cyber-based threats. In May 2021, the President issued E.O. 14028, "Improving the Nation's Cybersecurity," which mandated the implementation of certain additional security measures that will modernize federal government cybersecurity, enhance supply chain security, and improve the detection of vulnerabilities and incidents on federal government networks.

Additionally, the newly created Office of the National Cyber Director (ONCD) will play an important role in coordinating the U.S. Government's cybersecurity policy and strategy. The National Cyber Director is tasked with (1) ensuring federal coherence, (2) improving public-private collaboration, (3) aligning resources to priorities, and (4) increasing present and future resilience. The Department has met repeatedly with ONCD, including standing meetings among Department leadership and the National Cyber Director. The Department also has assigned attorneys for secondment to ONCD. Implementing more interconnectivity throughout the Department and ONCD will further the Department's cybersecurity resilience.

The Department also works and should continue to consult with other government agencies responsible for protecting the nation's cybersecurity. For example, the Department of Justice is working with CISA to ensure better information-sharing about suspected and identified attacks on the Department's computer systems. The Department recognizes that cyber threats require a whole-of-government response, whether that is in identifying vulnerabilities, responding to attacks and intrusions, or assessing the damages caused by a breach.

The Department should also place particular emphasis on ongoing exercises designed to self-assess its adherence to its internal cybersecurity

standards. Certain recent measures have placed greater emphasis on these exercises. For example, in October 2021, the Department completed its annual report as required under the Federal Information Security Modernization Act of 2014 (FISMA). One portion of this exercise, prepared by the Office of Inspector General (OIG), identified areas for improvement within the Department at six evaluated components. Recognizing the importance of these recommendations, in October 2021 the Deputy Attorney General directed the audited components to complete corrective action plans to address the areas for improvement identified by the OIG. Components must report on their progress to the Chief Information Officer (CIO) and Office of Privacy and Civil Liberties (OPCL), who are required to provide status reports to the Office of the Deputy Attorney General every sixty days. Additionally, in November 2021, at the direction of the Attorney General, the Deputy Attorney General issued a memorandum to all component heads—not just those subject to the recent FISMA review—directing them also to review the latest FISMA reports, identify any recommendations that should also be implemented within their component, and develop an implementation plan to address those areas.

In addition to protecting its own information, the Department will lead the effort to enforce cybersecurity requirements on federal contractors and grantees, leveraging its experience and expertise in civil fraud enforcement and other authorities. The Department's own conduct helps set standards across the nation and that it must lead by example in the way it protects vital networks and data. The Department will hold itself to the same standards that it expects others in critical infrastructure and other private sector industries to follow.

1. Safer Network Security

The Department, principally through the Office of the Chief Information Officer (OCIO), is working to implement a significant number of technical measures to improve the Department's network security—both to reduce the chances of future significant compromises and to better position the Department to respond should a compromise occur. Many of these improvements overlap and align with directives from E.O. 14028, which sets forth new security standards for all government agencies.[lxix] Others are based on interim recommendations made during the course of this review.

Zero Trust Architecture: Consistent with the directives set forth in E.O. 14028, the Department will continue to expeditiously implement a common Zero Trust Architecture across all components' unclassified information systems, thereby enabling secure user-based access to any Department system.[lxx] Zero Trust Architecture assumes that a breach is inevitable or has likely already occurred, so it limits access to only what is needed and looks for anomalous or malicious activity. Zero Trust Architecture embeds comprehensive security monitoring; granular risk-based access controls; and system security automation in a coordinated manner throughout all aspects of the infrastructure to protect data in real-time within a dynamic threat environment.

In July 2021, OCIO finalized its Zero Trust Implementation Plan, which outlines a comprehensive strategy to modernize the Department's cybersecurity architecture. The Department's modernization plan follows four phases: (1) creating a central identity and endpoint detection and response system, which will allow IT security teams to identify malicious

activity among normal user behavior; (2) overhauling the Department's internet access and virtual private network (VPN) systems to reduce external points of vulnerability; (3) implementing granular internal application access controls, in effect installing internal perimeters within the network; and (4) implementing internal application segmentation, thereby restricting the ability to move laterally within the network. This modernization plan has already begun but will continue to require significant resources (including additional funding from Congress) and support from Department leadership.

In order to ensure the Department continues to implement the modernization plan as quickly as possible, Department leadership should require routine updates from the OCIO on its progress implementing the Zero Trust Implementation Plan. These updates should identify any reasons for failing to meet the benchmarks, the implications of those failures in terms of timeline implementation, and proposed corrective plans to ensure updates.

Multifactor Authentication: Multifactor authentication is a critical and increasingly common security feature—for example, the one-time code sent to your phone to access an account, or the PIN associated with a bank card. The Department has used multifactor authentication for years on most of its systems, including the use of Personal Identity Verification credentials (commonly known as "PIV cards") and one-time randomly generated codes. The Department, therefore, is largely compliant with E.O. 14028's directive that all agencies adopt multi-factor authentication as a baseline security measure.

During the comprehensive review, however, the Department identified specific areas for improvement among its multi-factor authentication practices. One place to improve, for example, is in the use of PIV card multi-factor authentication, as opposed to authentication based on algorithm-generated codes. Among other reasons, PIV-based authentication is harder to compromise than other types of phish-able multifactor authentication in certain scenarios.[lxxi] Additionally, the Department's common use of PIV cards will ease the ability to use other forms of secure communications, including PIV-based encryption to send and receive encrypted emails. The Department is already increasing its use of PIV-based multi-factor authentication and should continue to improve this area of resilience.

During the course of the review, OCIO also noted an increased use of temporary exceptions to multi-factor authentication, which was partially attributable to the Department's sustained maximum telework posture during the COVID-19 pandemic.[lxxii] While the use of a small number of very limited exceptions seems advisable to continue Department operations, exceptions must be extremely constrained, and excepted systems should remain monitored for signs of compromise. To ensure that exceptions are no longer than necessary, the Department should promulgate policies that limit the use of exceptions. Such policies should include (1) limits on the duration for which an exception can be granted; (2) restrictions on the number of exceptions a single employee may receive during a specified period of time; and (3) regular reporting to a component's leadership about the use of exceptions.

The implementation of more PIV-based authentication and the restriction of MFA exceptions are both areas where corrective actions would require comparatively fewer resources than other network defenses. Department leadership should direct components to complete these improvements by the end of the year or otherwise explain why such protocols are not possible. In order to maintain visibility, components should provide regular reporting on

their progress. Additionally, each component's leadership should receive regular reports on how often exceptions are granted.

Data at Rest Encryption: Data at rest—data that is stored on Department laptops, thumb drives, servers, and other systems—is vulnerable to exposure not just through hacking, but also theft and loss of devices. For these reasons, E.O. 14028 mandates that all government agencies encrypt 100% of their data at rest. The Department has long encrypted at-rest data for many systems—laptops, flash drives, and devices commonly made mobile—but work remains to protect data on remaining systems. While the Department continues to work on its plan to implement data at rest encryption, all affected components should continue to provide Department leadership with routine updates on their corrective action plans.

As part of the remediation plans developed in response to the recent FISMA evaluation, all components were required to develop corrective action plans to address systems that do not currently employ data-at-rest encryption. Pursuant to the Deputy Attorney General's directive from November 2021, components shall continue to provide regular updates to OCIO on the status of their implementation of the corrective action plans. Additionally, all component heads should be directed to provide regular updates to the Office of the Deputy Attorney General on the status of their respective components' data-at-rest compliance.

Cloud Computing: E.O. 14028 calls for the federal government to accelerate movement to secure cloud services and for all federal agencies to prioritize resources for the adoption and use of cloud technology. To that end, the Department of Justice reviews its technology investments for secure cloud-readiness, cost-effective adoption strategies and overall cloud governance. The Department has already closed 99 of its 110 data centers and is tracking towards its goal to consolidate the remaining eight facilities by the end of FY 2022. Over the past few years, the Department grew its cloud storage by over 300%, with over 40% of all agency servers now in the cloud. The OCIO should continue to update leadership on its progress and promptly report any delays in the transition.

Enhanced Logging: Information from logs on Department networks and information systems can provide information invaluable for the detection, investigation, and remediation of cyber threats. The Department's 2020 Breach underscored the importance of maintaining such visibility before, during, and after a cyber incident.

E.O. 14028 calls for enhanced logging requirements as prescribed by the Office of Management and Budget (OMB). On August 27, 2021, OMB issued additional guidance about the necessary logging standards that government agencies should implement in order to be effective.[lxxiii] OMB's guidance included direction for agencies to assess the maturity of their logging practices, as well as to develop plans to achieve basic logging practices (as defined by OMB's guidance) by August 2022 and advanced logging practices by August 2023.

The Department has completed its assessment of its own logging practices and identified additional measures that would be necessary to achieve the OMB-set standards. The requirements are substantial and will take multiple phases to complete. The Department is prepared to take the necessary steps to begin this massive undertaking should the necessary congressional funding become available. Given this significant resource allocation, Department leadership should present these estimates to ONCD and CISA for further discussions about the path forward.

Mobile Device Security and Approved Applications: The Department's administration of mobile devices is currently managed at the component level. In this process, each component has developed different policies governing the permissible and impermissible applications that personnel are allowed to use on devices, as well as the means by which those rules are enforced. This inconsistent approach poses an increased risk of vulnerability due to the use of unsafe applications.

Certain components already use a "white-listing" process under which applications must be preapproved by relevant information-security personnel prior to their use on Department mobile devices. The remaining components should adopt a similar "white-listing" process, as well as clear guidelines outlining that mobile devices with unapproved applications will be suspended unless the unapproved applications are removed.

Additionally, so long as the Department's mobile devices continue to be managed at the component level, the Department should institute a way to compare the lists of approved applications that each component has permitted on its devices. This could be done for example, by having OCIO routinely collect from all components the list of approved applications and compare the lists across the components. Where there are notable discrepancies, OCIO should arrange for components to discuss the relative vulnerabilities of any application for which there is disagreement.

Email Systems Security: In the wake of the incident arising from the 2020 Breach, OCIO has conducted a comprehensive review of its email systems to identify ways in which its email system was particularly vulnerable to the compromise. Based on this review, OCIO developed additional remedial steps to limit the number of global administrators with access to email systems, increase the auditing of email systems, and increase login monitoring. OCIO continues to work with private vendors to identify ways to limit the largescale exploitation that occurred during the incident.

The Department should ensure that these improvements are integrated into all Department email systems, not just the ones maintained by OCIO. To that end, OCIO should share their remediation strategies with all individuals responsible for Department email systems. Those individuals, in turn, should assess whether the same steps need to be taken on the systems that they maintain. All components should report to leadership on the findings of their own analysis.

Network Compatibility: Responsibilities for the Department of Justice's network security are largely distributed among the Department's numerous offices, sections, and agencies that fall within the Department. Each of these Department components has significant autonomy in setting security protocols followed by that component, as well as the way in which the component monitors its systems for intrusions and compromises. While OCIO supports the successful execution of component missions, in practice OCIO has restricted visibility into some components' systems and limited ability to make operational decisions about component systems.

The devolution of responsibilities for network security has led to inefficiencies and incompatibilities. Prosecutors who work daily with FBI, Bureau of Alcohol, Tobacco, Firearms, and Explosives, or Drug Enforcement Administration agents routinely cannot access their own computer networks from law enforcement offices, and vice versa. Agents and attorneys often cannot work off the same workshare sites or communicate through secure message and videoconference applications,

adding levels of complication to investigative and prosecutorial reviews. Agents and Department prosecutors sometimes operate on different encryption platforms, hindering the ability to communicate easily and forcing them to use either more cumbersome methods or forego the additional security layers. Segregated networks across the Department also limit the ability of security specialists to have visibility across the panoply of Department networks, creating areas in the network where they cannot be as vigilant because fewer proverbial eyes guard the space.

The Department often operates best when members of the different components work shoulder-to-shoulder in a team model—prosecutors directly embedded with agents to work high-profile matters, and agents from different law enforcement components working on task forces. The Department's digital setup should mimic the physical arrangement. The Department has initiated a study to build further interoperability of networks. This work should continue with the support of Department leadership, with specific representatives from each component assigned to study the issue and with responsibilities to form specific recommendations by the end of the fiscal year.

To realize potential efficiencies in the Department's procurement process for network security software and hardware, the CIOs of Department components need to collaborate to identify licenses or hardware for which an enterprise license or other arrangement would be significantly less expensive and allow easier integration. Coordination also will increase the likelihood that contracts contain uniform provisions for certain cybersecurity requirements and that procurement officials share information about reported breaches or continuous monitoring reports that may be required by a contract.

2. Safer Electronic Communication

The Department needs to continue to improve its culture regarding the handling of unclassified case-sensitive and other similar information. Many attorneys, agents, and other Department personnel routinely receive and send information electronically that, although unclassified, implicates covert investigations, the safety of cooperating witnesses, and other highly sensitive subjects. While email, text messages, and other forms of electronic communication are efficient forms of communication, they are vulnerable to the sophisticated adversaries that are targeting its systems. The Department cannot let the speed of communication come at the cost of appropriate safety measures.

Improving the handling of sensitive Department information requires both technological and educational improvements. Educationally, the Department has already increased the training that employees receive to ensure familiarity with the suite of tools that will allow secure transfers of data. For the first time ever, the Department required that personnel take specific training on the types of available encryption tools that were available to safely transmit documents. Department personnel must understand that unencrypted email is a system that is relatively unsafe compared to other forms of transmission. Technologically, the Department needs to continue to develop new encryption and data-security methods that are user-friendly and not unduly burdensome, to incentivize higher usage of such tools.

In general, Department employees are over-reliant on the transmission of sensitive Department information through email without the use of encryption. Even when unclassified, Department personnel routinely handle sensitive

information that is of significant value to foreign adversaries and cybercriminals. Likewise, the Department routinely transmits information that, if disclosed, could jeopardize investigations, law enforcement actions, and the safety and privacy of individuals. While the Department already has tools to share information through more secure channels, usage of those tools remains relatively low in part due to the increased burden of using these tools over insecure email.

Similarly, Department employees need to carefully consider how they share and transfer information outside of the Department. Law firms, courts, and other participants in the judicial system have historically been targeted by cyber actors in part because they have access to Department information that bears on sensitive operations and cases.

Handling and Transmission of Sensitive Court Filings

On January 6, 2021, the Secretary of the Judicial Conference issued a policy change advising that federal courts should (1) accept filings of Highly Sensitive Documents (HSDs) only when they are submitted in paper form or via a secure electronic device; and (2) store HSDs in a secure paper filing system or on a secure, standalone computer system not connected to the internet or any network. This policy would preclude filing or storing HSDs within the Case Management/ Electronic Case Filing (CM/ECF) system. The Secretary of the Judicial Conference issued this guidance based on a DHS audit of CM/ECF that identified serious security vulnerabilities and an apparent compromise that risks unauthorized access to documents stored on the system. An investigation into the apparent compromise of CM/ECF is ongoing.

The Department takes the risk posed by the CM/ECF vulnerability seriously and has taken several steps to address it. In January 2021, the Principal Associate Deputy Attorney General issued a policy on electronic filing of Highly Sensitive Materials.[lxxiv] This guidance included factors for Department attorneys to consider when assessing whether a filing may qualify as an HSD and thus require secure filing outside of the CM/ECF system. Department and FBI leadership subsequently provided a comprehensive classified briefing to U.S. Attorneys or their designees about the risks that the CM/ECF vulnerability may pose to ongoing litigation as well as best practices regarding the HSD policy.

Since the vulnerabilities were detected, the Department, through EOUSA and NSD, have provided further guidance to U.S. Attorneys and their senior staff on the HSD policy. NSD has also provided support and recommendations to the U.S. Attorney community on how best to address issues that arose on a case-by-case basis. The Department is also advising the federal judiciary branch's new cybersecurity task force on ways to improve its security.

3. Protocols and Policies for Breach Incidents

Department personnel routinely use its unclassified servers, networks, and applications to diligently further the nation's interests across these broad areas of responsibility. While these technologies have greatly enhanced the Department's ability to serve the American people, they also make the data contained therein potentially vulnerable to compromise. As the 2020 Breach demonstrated, adversarial groups are taking unprecedented steps to gain access to the Department's unclassified network. There is no indication that these adversaries will relent. It is therefore necessary for the Department to develop protocols and policies that anticipate, prevent, and properly remediate any harm that a potential breach would cause.

Responding to a cyber incident is not just the responsibility of the CIO or CISO. Instead, the Department must engage in a multifaceted effort that goes beyond the immediate response to the breach. To that end and as part of the comprehensive review, the Department is developing a Justice Cyber Incident Playbook (JCIP). The JCIP is designed to provide senior Department leadership with a comprehensive guide on best practices in responding to a cyber incident affecting the Department's systems. The Plan focuses on four main goals: (1) cyber defense; (2) assessment and notification; (3) investigation of the breach; and (4) operational remediation. While the JCIP is focused on the needs of Department leadership, it can serve as a template for component-level breach response plans, which would in turn allow the Department to have a more modular approach to a cyber incident that activates plans focused on the impacted components.

A successful cyber incident response plan cannot rely on the innate expertise of the leadership organizing the response. The JCIP is thus designed as an accessible document that will allow Department and component leadership to promptly and effectively respond to a cyber incident, even if they lack expertise in this area. The JCIP includes a timeline of important steps that the Department must take when responding to a cyber incident. It also includes sections analyzing notification requirements, initial investigative steps, operational risks, and legal issues that senior Department leadership may need to consider as a result of a breach. Finally, the JCIP's appendices provide definitions of key terms, a directory of essential Department actors who may need to be consulted during a cyber incident, and a list of essential authorities.

In addition to notifications mandated by statute or regulation, the JCIP also includes a section on prudential disclosures, along with analysis of the situations when engaging in these disclosures is appropriate. The JCIP will thus also help the Department to better integrate itself into a whole-of-government and whole-of-society response where information sharing is critical for collective defense.

The review also noted that the Department needs to better understand what data should be regarded as most sensitive. The federal government is migrating from a perimeter-based view of cybersecurity to one that anticipates sophisticated intrusions onto its networks. As part of that strategy, CISA, the National Institute of Standards and Technology (NIST), and other agencies are encouraging departments to identify essential data and devote greater resources toward defending them, as set forth in Federal Information Processing Standards Publication 199 (FIPS 199). The identification of "high impact information," as defined in FIPS 199, achieves that goal by focusing on any unclassified information that is essential to the Department's core functions that, were an adversary to gain access to it, could have a debilitating impact on the Department's mission, or otherwise result

in significant harm to individuals, American businesses, or government interests. As part of the process, the Department should assess high impact information on its network, increase protections for this essential data, and create component-level remediation plans to address harms were an adversary to nonetheless gain access to it.

The focus on FIPS 199 high impact information will allow the Department to properly allocate its resources to protect truly essential information, rather than a diffuse approach that accords roughly equal value to all data and in turn reduces cyber readiness.

4. Contractor and Vendor Cybersecurity

Like the rest of the U.S. government, the Department relies on numerous contractors and outside vendors to provide critical services. Some contractors—such as those that provide technical or specialized assistance in investigations—routinely handle sensitive evidence, either on their own systems or Department networks. Other contractors are responsible for holding sensitive Department data about the workforce. The Department likewise relies on vendors to provide hardware and software for a variety of purposes, from maintaining the Department's networks to the tools used to process and examine digital evidence.

As demonstrated by the 2020 Breach, a compromise of a vendor or contractor can have significant deleterious effects. The initial compromise of SolarWinds was a supply-chain attack on a vendor that was compounded by the compromise of email systems being run on vendor-supplied software.[lxxv]

The Department must therefore ensure that contractors and vendors follow appropriate cybersecurity practices, so that these partners do not become a weak point through which the Department is compromised. Mandating effective cybersecurity practices requires that the Department promulgate standards that are clear, effective, and enforceable. Component procurement executives must work with their CIO counterparts and/or the Department OCIO to ensure that the appropriate cybersecurity and supply chain risk management clauses are incorporated into all solicitations and contract documents.

To that end, the Department continues to further integrate privacy and security risk assessments into IT budget and capital planning processes, as well as privacy and security terms and conditions into the Department's general procurement documents, templates, and contracts.

Once provisions are clear and effective, the Department should integrate and deploy a significant number of the tools at its discretion to ensure contractual cybersecurity standards are followed. These include termination of contracts for failure to follow appropriate cybersecurity standards and, in cases of reckless or intentional failure to maintain cybersecurity standards, civil enforcement actions that carry significant monetary penalties.

A. Updated Cybersecurity Standards for Federal Contractors

During the review, many of the cybersecurity provisions and standards set forth for federal contractors were found to be insufficiently rigorous. Likewise, E.O. 14028 provides for a process to update contract requirements and language for contracting with service providers, a process that will be led by the Federal Acquisition Regulation (FAR) Council with input from OMB. Given the Department's responsibility for enforcing such contracts, the Department's Civil

Division has offered to assist in the development of these terms in order to ensure such standards are enforceable.

Separate from efforts to update government-wide contractor and vendor provisions, the Department should continue to undertake multiple lines of efforts to update its own requirements for vendors and contractors. These efforts include: (1) updating the Justice Acquisition Regulation (JAR) requirements for IT-related procurement, in order to ensure adequate cybersecurity standards are followed; (2) conducting a review of existing contracts for inadequate cybersecurity measures; (3) implementing a mandatory privacy clause in internet technology procurements, to ensure that sensitive Department data is protected; (4) mandating privacy reviews of high-dollar or high-risk procurement proposals; and (5) implementing a privacy clause in Department procurements through Acquisition Policy Notice 21-07. These efforts, currently undertaken by the Justice Management Division (JMD), OCIO, and OPCL, will both supplement government-wide enhancements currently undertaken through the FAR process and can serve as a stopgap measure while the FAR process continues.

B. Civil Enforcement for Cybersecurity Fraud

In some circumstances, a contractor's or vendor's failure to follow agreed-upon cybersecurity precautions could constitute fraud against the Government. The Department of Justice possesses various civil tools to pursue such fraud, including civil statutory remedies for fraud against the government under the False Claims Act.[lxxvi] The Fraud Section of the Civil Division's Commercial Litigation Branch has the Department's principal expertise in civil fraud litigation.

> *"For too long, companies have chosen silence under the mistaken belief that it is less risky to hide a breach than to bring it forward and report it. Well, that changes today."*
>
> DAG Lisa O. Monaco, Press Release Announcing New Civil Cyber-Fraud Initiative (Oct. 6, 2021)

In October 2021, the Deputy Attorney General and Acting Assistant Attorney General for the Civil Division announced the Civil Cyber-Fraud Initiative (CCFI), which uses the Department's authorities under the False Claims Act to pursue civil actions against government grantees and contractors—including those under contract with the Department of Justice—who fail to meet cybersecurity obligations.

Given the Civil Division's increased responsibility in enforcing cybersecurity standards, it should also play a significant role in revising and developing operable contract and procurement provisions. Prior to the publication of the Justice Acquisition Regulation, OCIO and JMD Procurement should ensure that the proposed revisions are reviewed by the Civil Division's Fraud Section to ensure the new provisions are enforceable in the case of breach. Likewise, the Department should also endeavor to ensure that the Civil Division is consulted during the FAR Council-led revisions to similar government-wide provisions.

Civil Cyber-Fraud Initiative

In October 2021, Deputy Attorney General Lisa O. Monaco announced the launch of the CCFI, led by the Civil Division's Commercial Litigation Branch, Fraud Section. The CCFI combines the Department's expertise in civil fraud enforcement, government procurement and cybersecurity to combat new and emerging cyber threats to the security of sensitive information and critical systems.

The CCFI utilizes the False Claims Act to pursue cybersecurity-related fraud by government contractors and grant recipients. The False Claims Act is the Government's primary civil tool to redress false claims for federal funds and property involving government programs and operations. The Act includes a unique whistleblower provision, which allows private parties to assist the Government in identifying and pursing fraudulent conduct and to share in any recovery and protects whistleblowers who bring these violations and failures from retaliation.

The CCFI will hold accountable entities or individuals that put U.S. information or systems at risk by knowingly providing deficient cybersecurity products or services, knowingly misrepresenting their cybersecurity practices or protocols, or knowingly violating obligations to monitor and report cyber incidents and breaches. The benefits of the initiative will include (a) building broad resiliency against cybersecurity intrusions across the government, the public sector and key industry partners; (b) holding contractors and grantees to their commitments to protect government information and infrastructure; (c) supporting government experts' efforts to timely identify, create and publicize patches for vulnerabilities in commonly-used IT products and services; (d) ensuring that companies that follow the rules and invest in meeting cybersecurity requirements are not at a competitive disadvantage; (e) reimbursing the government and taxpayers for the losses incurred when companies fail to satisfy their cybersecurity obligations; and (f) improving overall cybersecurity practices that will benefit the government, private users and the American public.

The CCFI is being led by the Civil Fraud Section and implemented by a working group of Civil Division attorneys, Assistant U.S. Attorneys, and representatives from nineteen federal agencies. Agency representatives include agents, auditors, and attorneys from the agencies' respective OIGs. The Department has already received numerous referrals that remain the subject of ongoing Department investigations.

IV. ADDITIONAL PRIORITIES AND VALUES

This review also considered two sets of issues that implicate not just the ongoing evolution of digital technology, but how the Department accounts for those inevitable developments while retaining its values and capabilities. The first issue is how the Department accounts for the development of new technologies—not only what risks they might pose to the nation, but also how they would implicate the Department's own operations. The second issue is how the Department can maintain its expertise and workforce on cyber-related matters.

1. Emerging Technologies

Emerging technologies will continue to pose new issues—whether those technologies are abused for unlawful purposes or used by the Department in aid of its investigations and other operations. The Department must proactively anticipate the consequences of emerging technologies before they become mainstream, or else it will risk being ill-positioned to deal with them in a timely fashion. Numerous parts of the Department already contemplate the implications of over-the-horizon technologies.

When it comes to its own use of certain new technologies, the Department has developed frameworks and promulgated guidance. For example, in November 2019, the Department's Office of Legal Policy published an updated policy on the Use of Unmanned Aircraft Systems (UAS), which enables the Department of Justice's law enforcement components to safely and responsibly employ UAS technology within a framework designed to provide accountability and protect privacy and civil liberties.[lxxvii] These reviews and frameworks, however, have been *ad hoc* and sparked by outside prompting, such as Executive Orders.

The review found that while numerous parts of the Department are evaluating and working on emerging technologies, their efforts are disparate, duplicative, and uncoordinated. Further, existing Department policy requiring completion of initial privacy assessments is not consistently followed. The result is that the Department is not as efficient or effective at thinking about emerging technologies as it could be, nor is it as fast as it should be to establish guidance and policies about the Department's own use of such technologies. As recommended below, a standing interdisciplinary body within the Department with responsibilities for identifying emerging technologies would help streamline efforts to consider their implications, as well as ensure that the totality of the Department's institutional knowledge and diversity of perspectives is captured in these reviews.

The absence of such a standing body, however, has not prevented the Department from looking at a host of new emerging technologies and tools that require immediate further action from the Department. These include artificial intelligence (AI), third-party surveillance and search tools, and big datasets, including those that are commercially available. These efforts should continue, particularly in making sure the Department has policies in place, and is enforcing compliance with existing policies such as initial privacy assessment (IPA) completion, to guide its own use of such technologies.

Emerging Technology Board: Given the numerous possible issues that could arise with over-the-horizon technologies, the Department has always monitored emerging technologies for their ramifications on the Department's work. Potential consequences of new technologies extend well beyond concerns about ensuring that the Department's components efficiently invest in and use data assets and that such components' existing data management programs effectively and efficiently handle the data such technologies produce. The Department is already well positioned to manage such issues through its existing Data Governance Board (DGB). The Department should also ensure a whole-of-Department alignment of security, investigative, privacy, civil rights, and artificial intelligence interests implicated by emerging technologies.

Historically, CCIPS and the Office of Enforcement Operations (OEO) have borne principal responsibility for identifying emerging tools and technologies that require proactive thinking. Looking forward, this long-term analytical work would benefit from an expansion and formalization to include representatives from a wide variety of components. Thus, the Department should form an intradepartmental **"Emerging Technology Board"** (ETB) tasked with advising Department leadership about nascent technologies, emerging threats, opportunities, and related legal, policy, and resource issues impacting the Department's cyber work. The ETB should coordinate and optimize a whole-of-Department, best practices approach to emerging technologies, which requires, at minimum, input from CRM, NSD, CRT, the Office of Legal Policy, OCIO, OPCL, and all law enforcement component representatives. Such a diversity of viewpoints would ensure that the Department benefits from a significantly broader perspective than before.

The ETB should meet regularly to (1) identify technologies that are likely to impact the Department's work; (2) consider issues that are likely to be significant to the Department vis-à-vis relevant technology, both in terms of others' use and in terms of the Department's use of such technology; and (3) develop a workplan to coherently address those different lines' potential effect. The ETB should regularly update the Department's leadership about these lines of effort and, where appropriate, develop guidance for the Department on such technologies. Rather than supplanting any existing lines of effort to study emerging technologies, the ETB should ensure disparate lines of effort are coordinated within the Department.

Artificial Intelligence: AI—here used to describe the suite of emerging technologies in which a computer automates complex tasks associated with human intelligence—offers significant promise for the Department of Justice. AI programs already offer the ability to identify relevant documents among a sea of corporate records, match the facial features of a terrorism suspect to other government holdings, and identify victims in cases of online child sexual exploitation. The applications of AI will only grow in the future.

The promise of AI, however, comes with attendant risks. In certain cases, some AI applications may have implicit biases in their coding or construction, which could undermine the work of the Department. Other novel applications will initially emerge before courts have a chance to consider their constitutional and statutory implications—for example, whether the use of such applications requires legal process or predication in order to protect the individual right to privacy.

The Department, through the ETB and pre-existing workstreams (e.g., within the DGB and CRT), needs to be thoughtful about its use of AI tools, both on case-by-case and routine bases. It should also ensure that Department components anticipate and work to mitigate possible pitfalls in using those tools. This analysis ideally should occur during the development process or before the procurement of such tools, follow existing Department policy such as the completion of initial privacy assessments, and involve periodic reviews of the use and utility of these new emerging technology tools to understand what unanticipated issues may arise in practice.

The relevant Department stakeholders also need to anticipate how AI technologies may lead—deliberately or unintentionally—to abuse and violations of federal civil and criminal laws. The Department, led by CRT, is already studying how AI may cause or exacerbate unlawful practices that disadvantage specific protected groups or cause unequal access to law.

The Department's DGB implements the Department's 2019 Data Strategy specific to AI matters through the 2021 AI Strategy Implementation Plan. The Department's AI Community of Interest (COI), chartered under the DGB, serves as the principal Department-wide forum for uniting DOJ employees around AI technology, standards, policy, programs, and acquisition. The AI COI facilitates knowledge sharing across all Department components in order to accelerate deployment and appropriate use of AI in accordance with the AI Strategy, and provides a forum for coordinating AI initiatives, facilitating implementation of Department-wide AI processes and standards, and addressing common AI issues or concerns among components.

As a first step to address Department governance of AI, the Department's AI COI, with the input from AI COI members and representatives of Department Bureaus, Officers, Boards, and Divisions, is completing the Department's first-ever Principles for the Ethical Use of Artificial Intelligence ("the Principles"). The Principles establish guidelines for all AI activities, implement relevant Executive Branch orders and guidance to date, and charge components with developing and implementing specifically tailored policies and procedures to guide their use of AI consistent with the Principles, the overall DOJ AI Strategy, and the Department's mission. Advances in the field of AI as well as new law, regulation, policy, and guidance will continue to shape the Department's use of this emerging technology. To ensure the Principles evolve alongside its understanding and use of AI, the Department will closely monitor and review the AI landscape and update the Principles as appropriate to ensure responsible and ethical design, development, acquisition, and use of AI, with appropriate leader visibility. Department leadership will publish the Principles on the Department's website.

The Department should use the newly developed Principles to assess the current and future uses of AI systems. To that end, the newly created Emerging Technology Board should include in its review the ongoing and contemplated uses of AI systems by the Department, based on the Principles and any other operative federal or Department policies. This review would dovetail with an existing directive that each agency complete an inventory of its non-classified and non-sensitive use cases of AI, in accordance with guidance issued by the Federal Chief Information Officers Council (Federal CIO Council).

The Department also has an important voice in the development of AI systems, particularly those that threaten to perpetuate past discriminatory practices by incorporating, and then replicating or amplifying historical patterns of inequality. Without careful consideration, AI systems used in various private sector industries may very well exacerbate discriminatory practices in housing, employment, healthcare, and other fields. As entities increasingly rely on algorithms to make decisions, their decisions become increasingly difficult to challenge because the underlying processes are opaque. This lack of transparency and accountability raises serious concerns about inaccuracy, and also opens the door to potential discrimination. The Department should proactively engage with designers and developers, as well as those who use AI systems, to discuss the potential unlawful and discriminatory ramifications and how such effects can be avoided.

CRT is identifying where coordination and engagement with other federal agencies and stakeholders might be most effective. To that end, the Division should continue coordination and outreach efforts with other agencies, including with NIST, which is charged with developing technical standards and related tools for creating AI systems under guidelines that reduce the risk of discriminatory or biased effects.

Novel Third-Party Tools and Technologies: In recent years, an increasing number of third-party companies have developed new tools designed to, among other things, aid in cyber investigations. These tools' capabilities include accessing devices, locating criminal infrastructure, and otherwise assisting in the search for malicious activity across the internet. Used appropriately and pursuant to legal process, as necessary, these tools can greatly assist the Department in disrupting cyber threats and identifying those responsible. However, the proliferation of companies and tools carries attendant risks that the companies and individuals who create these tools are working at odds with the Department's values and overall mission, or could undermine the public's trust in the mission.

The Department should therefore (1) institute policy and process to weigh the totality of the costs and benefits in a systematic fashion; and (2) ensure that Department leadership—including the leadership offices of relevant law enforcement components—maintain visibility into the tools being both used and contemplated for use, as well as the third-party entities that create them. Leadership should exercise an involved role in deciding whether there should be restrictions on the types of investigations for which such tools are deployed.

The Department should have a comprehensive set of guidelines governing the procurement or use of a new third-party tool or technology. These guidelines would include, among other things, the possibility that the tool has a vulnerability or could otherwise jeopardize the Department's IT systems; the impact from use of the tool on investigations and potential future prosecution; what testing the tool will undergo before deployment, and under what controls (*e.g.*, in a controlled environment that does not impact Department IT systems or the internet); what, if any, reputational risks the tool poses to the Department; whether legal process will be required before operationally using the tool; and whether the tool is duplicative of existing capabilities within the Department, or within the U.S. Government. These guidelines, while advisory, will incorporate and draw from experiences and expertise from across the Department—from the law enforcement and litigating components to its procurement specialists and security officers.

The purchase and use of novel third-party tools and technologies can sometimes be a relatively straightforward process. Given the variety of potential issues that can arise from the use of a new tool, however, controls and procedures should be put in place, and compliance mechanisms established, to ensure an appropriate level of supervision over such new technologies exists, while still allowing Department personnel to explore new tools and methods to lawfully and responsibly accomplish the Department's mission.

Big Data: Both private and public actors continue to amass and aggregate significant amounts of data. The aggregation and analysis of this data can provide valuable investigative leads in a range of cases, from cyber threats to counterterrorism to corporate crime. Likewise, the Department already uses data analytics to assist in investigations of healthcare fraud, securities fraud, and various national security investigations. The Department needs to continue to identify opportunities to amplify its investigation through the appropriate and considered use of data-driven investigations.

At the same time, the Department, coordinated through the ETB, needs to consider carefully what data it collects—both the lawfulness of the sources and the veracity of the data itself. Unreliable data or analytics can lead to wasteful delay, incorrect identification of sources, and other issues. Third-party sources of data can be collected in ethical or unethical ways. Some datasets can be incomplete or inaccurate such that they lead to unintentionally biased results when analyzed. Moreover, the Government's use or interest in such data can establish perverse incentives among private actors, who may collect such data using unlawful, unethical, or biased manners and means (including manners and means that infringe on the intellectual property of well-meaning companies or relationships of trust with their customers). Prior to entering into business agreements with third-party commercial sources, the Department must engage in reasonable due diligence to ascertain that the commercial sources acquired the data using lawful and ethical means. These efforts should be documented in the initial privacy assessments.

The DGB is the principal internal Department forum for addressing the Department's data management standards, priorities, and practices. The DGB serves as the leader for coordinating and facilitating implementation of Department-wide processes and standards, and for addressing common issues affecting component data programs and resources. The DGB includes representation from the subject matter experts who share accountability for the effective development and execution of data architectures, policies, practices, and procedures including the Department Chief Data, Statistical, Evaluation, Financial, Procurement, Legal, Privacy, Records, Information, Technology, and Cyber Security Officers, and the component data stewards, system owners, and records managers. Together, they implement the Department's "Data Strategy."

The Data Architecture Working Group (DAWG) supports the DGB and executes the Department's "Data Strategy Implementation Plan," with a focus on data management and information sharing. The DAWG is a stakeholder of the Department's "Justice Data Catalog," an internal Department application that provides a central inventory of all datasets collected throughout the Department. The Justice Data Catalog defines standardized metadata for data sets, increases awareness of data available throughout the Department, encourages cross-component community of interest and collaboration, aligns with the Department's

Data Strategy for streamlined data management, sharing, and reuse, and enables disclosure, as appropriate, of the Department's open data to the public via Data.gov integration.

Given the number of components and offices that may be interested in harnessing datasets, the Department should look collectively to (1) increase its overall capacity to handle and analyze large data sets; (2) establish guidance for how to collect, retain, and analyze data sets in commonly encountered big data settings—including the sources used to collect data, the way data is stored and accessed, and the ways in which it is used to further investigations and other operations; and (3) establish guidance specific to how the Department needs to conform its collection and handling of big data in light of Constitutional protections such as those afforded by the First and Fourth Amendments.

2. Improving the Department's Cyber Workforce

The Department relies on a host of dedicated and talented personnel to respond to, investigate, and disrupt cyber threats—including attorneys, special agents, intelligence analysts, computer scientists, data analysts, forensic technicians, and others. These public servants reside in a variety of Department components and each subset brings unique expertise to the Department's efforts to disrupt malicious cyber threats.

In 1996, the CRM's CCIPS was established from an earlier five-attorney "Computer Crime Unit," first founded in 1991. Since that time, CCIPS has been the cornerstone of the Department's efforts to combat cyber and intellectual property crimes. CCIPS maintains the CCIPS Cybercrime Lab, which provides advanced digital investigative analysis, cybercrime investigative, and other technical support to Department prosecutors. Beginning in 2012, NSD has dedicated a small team of prosecutors to investigate and disrupt the nation state cyber threat. Since then, NSD's cyber-focused prosecutors, now housed in CES, have navigated the nexus between law enforcement and national security communities to have an outsized disruptive effect, as described in part herein. Starting in 2020, NSD initiated a sustained effort to increase the number of CES prosecutors dedicated to disrupting cyber threats.

Since 2002, FBI's investigations into cyber threats have been coordinated through CyD. CyD addresses all violations with a cyber nexus, which necessarily supports FBI priorities across program lines, assisting counterterrorism, counterintelligence, and other investigations when aggressive technological investigative assistance is required. CyD also ensures that agents, analysts, and other personnel with specialized technology skills are focused on cyber-related investigations.

The Department's investigative cyber expertise does not lie solely within the FBI, however. Since almost every area of law enforcement is now investigating crimes with cyber elements—whether they involve the use of darknet marketplaces or cryptocurrency laundering to funnel narco-proceeds back to traffickers—each of the Department's five law enforcement components maintains personnel with specialties in cyber investigations.

Separately, the Department relies on a host of technical architects, privacy professionals, cybersecurity experts, and IT specialists to architect, secure, and protect Department networks and systems. These professionals defend the Department's infrastructure from attacks by external parties as well as from insider threats. With the rapid proliferation of cyber threats, including ransomware and other malicious attacks, it is imperative these roles are filled with a highly qualified workforce.

To keep pace with the rapidly changing landscape, the Department must have appropriate personnel in place to understand both the technology and the potential applications. The Department needs prosecutors and investigators capable of understanding the technical details involved in sophisticated breaches and attacks, as well as the national security dimensions of certain actions that might appear purely criminal at first blush. Well-rounded cyber prosecutors therefore must have interdisciplinary experience in the applicable prosecutorial practices, as well as familiarity with the common tools used to investigate different types of threats, from individual criminals to nation-states. And the Department needs experienced cyber attorneys to represent the Department in National Security Council-led policymaking processes and coordinated interagency responses to significant cyber incidents.

To understand the personnel-related issues related to cyber matters, the review spoke with leadership in multiple U.S. Attorneys' Offices, the OCIO, OPCL, JMD, law enforcement components, and other relevant Department components. Most of the interviewed offices noted that the competition for talent in cyber specialties is significant, and the Department's reputation for high-quality work can only attract so much talent, especially in light of higher pay in the private sector and at other departments and agencies. The Department must consider what resources and tools it can use to attract and retain top-tiered talent, to carry out critical cyber investigations, prosecutions, and other mission-driven efforts as well as to ensure its network resilience.

Training and Capacity Building: As advancements in technology have affected every facet of its daily lives, malicious actors have found ways to harness technology to further a vast array of criminal activity. The growth of societal use of electronic devices, social media, and online communications has also led to the abuse of these same technologies, not only by cybercriminals, but also by narcotics traffickers who message their clients and co-conspirators from their smart phones; white-collar criminals advertising their fraudulent schemes to the public; and abusers who seek out and target their victims online. Yet, all forms of digital activity leaves behind a trail of information. Thus, the increased dependence of criminals of all stripes upon electronic devices and online platforms requires a concurrent capability of investigators across the Department to understand how to follow the digital footprints left behind by malicious actors in all of its cases.

Trial attorneys and Assistant United States Attorneys, upon joining the Department, should be required to receive basic training on (1) electronic evidence and discovery; (2) basic investigative techniques regarding stored communications, pen register and trap and trace devices, and wiretap techniques, and the legal and constitutional issues surrounding their use; (3) cryptocurrency and other digital assets; and (4) international evidence collection in furtherance of investigations. This training requirement may be fulfilled either through sessions offered by components or U.S. Attorney's Offices; by classes offered through EOUSA's Office of Legal and Victim Programs and the Office of Legal Education; or by trainings offered online or in person by subject matter experts from CCIPS, OEO, MLARS, OIA, and the NCET. Such training would ensure that every new attorney within the Department begins with a baseline understanding of the skills and techniques that are required to investigate crimes in this increasingly digital world.

In addition, in instances in which complex cyber and digital assets investigations have successfully implemented the strategies

highlighted herein, including the innovative use of all of the Department's available tools, and coordinated whole-of-government campaigns and international efforts, the Department should ensure that its cyber and digital assets specialists benefit from lessons learned. To that end, CCIPS, MLARS, OIA, CES, EOUSA, and the NCET should continue to identify techniques used and lessons learned in complex investigations for purposes of providing further capacity building within the Department. Such efforts should include but not be limited to increasing partnerships on investigations with Assistant United States Attorneys and trail attorneys in other components, continuing to provide guidance and exemplars of legal process and court filings, and presentations and case studies from subject matter experts on a regular basis.

Cyber Workforce Recruitment and Retention: Although the federal government has rapidly expanded its cybersecurity workforce in the last 15 years—for example, DHS has established an entirely new cybersecurity agency with a $3 billion budget, and DOD has created a new cyber command that now has more than 6,000 personnel—the Department's total number of cyber-specialized attorneys has remained roughly the same size over the last 15 years. CCIPS, in particular, has employed approximately 37 prosecutors since 2010, and has occasionally shrunk. Additionally, although this report references a large number of significant successes against national security cyber threats, until 2020, NSD's CES had approximately three prosecutors dedicated to investigating, disrupting, and deterring nation state cyber threats. Even accounting for the number of FBI cyber investigators, the Department has leveraged these relatively limited personnel numbers into an immense positive impact on this country's cybersecurity.

One of the reasons for the Department's outsized success against cyber threats has been its mission-driven workforce. However, the Department, including the FBI, is not immune from significant challenges in retaining its existing experienced cyber-specialized workforce. For example, although all Department attorneys are almost all paid less than their private sector counterparts, among cyber-specialized attorneys the problem is particularly acute, with even relatively junior attorneys being offered significant salary increases if they leave the Department and enter the private sector. It has become increasingly difficult to retain cyber-specialized attorneys after they obtain four or more years of experience working cyber investigations. The Department's other cyber-related personnel, including special agents, analysts, computer scientists, and IT and information security personnel, face similar compensation disparities between the Department and other employers. If not addressed, this problem will result in the Department effectively becoming a temporary waystation for cyber talent, rather than a viable long-term career option.

In the face of these disparities, government budget and personnel authorities have recognized the need for enhancements to the federal service's recruitment and retention efforts. DHS and DOD have both taken steps toward addressing similar problems by creating new types of Federal civil service positions for their cyber-specialized employees. Since 2016, DOD has been authorized to hire cyber personnel outside of the traditional civil service system through the Cyber Excepted Service Personnel System.[lxxix] In November 2021, DHS announced the Cybersecurity Talent Management System, which also allowed DHS's Cybersecurity Service to more effectively recruit, develop, and retain cybersecurity professionals. In some cases, DHS and DOD can pay salaries equaling that of the Vice President.[lxxx] Those

pay scales highlight that the Department's ability to compensate its cyber-specialized workforce lags behind not only the private sector, but also the public sector.

Additional cyber-specific pay incentives at other government departments and agencies have made it more difficult for the Department to fill its own important cyber personnel needs. For example, based on recent job postings, CISA is willing to pay a recent computer science graduate in the Washington, D.C. area approximately $95,000; the FBI, in turn, currently offers the same candidate a starting salary of approximately $64,000.[lxxxi] During an FY 2021 hiring push, the FBI issued almost 100 Conditional Job Offers to IT specialists and computer scientists. While 69 individuals initially accepted their offers, only 28 were onboarded in the fiscal year. Fifty-eight percent of those who ultimately did not onboard cited insufficient salary incentives as one of their reasons for declining the offer or accepting a position elsewhere.

Use of Cyber Hiring and Retention Authorities: The Department is not without options in addressing these cyber workforce challenges. For example, the Department should utilize general authorities established by Congress to draw technology-oriented talent in federal service. These include a government-wide direct hire authority for General Schedule (GS)-9 through GS-15 level positions in IT management and special pay rates for entry and developmental level computer engineers, computer science and IT specialists.[lxxxii]

The Department should also exercise non-cyber incentives. For instance, in certain circumstances, federal agencies can pay bonus compensation to recruit and retain GS and Senior Executive Service (SES) personnel.[lxxxiii] Under these authorities, DOJ components can offer up to 25% of basic pay as incentive compensation to new-hires in hard-to-fill roles.[lxxxiv] This incentive is available on an annual basis for up to four years, provided the candidate meets eligibility requirements. If there is reason to believe an employee in a hard-to-fill role would leave Federal Service, agencies can utilize similar retention incentives for up to 4 years. However, the Department must justify these recruitment and retention incentives for each employee on an annual basis. Federal agencies can also use the Superior Qualifications and Special Needs Pay-Setting authority to establish pay for new GS hires, if the Department demonstrates that the candidate has superior qualifications, or that it has a special need for that candidate's services.[lxxxv] Moreover, agencies can request that OPM establish special pay rates for a unique grouping of roles; those circumstances must be exceptional, and the authorities are typically narrowly applied. Other standard human resource incentives include relocation pay, loan repayment (up to $60,000 toward federally insured student loans) and increased leave accrual for non-federal and military experience. For certain positions, components can also hire personnel into SES roles.[lxxxvi]

Although these incentives are available across agencies, Department managers and employees are often unaware of their existence, unsure of their requirements, and lack guidance regarding their application in recruitment and retention efforts. Budget concerns exacerbate the hesitation to use such authorities, including that additional compensation is not factored into existing personnel projections (and could therefore result in hiring fewer people overall). Department managers that were aware of these compensation incentives noted fairness and perception concerns prevent their application. For example, maximizing the bonus for a senior cyber hire could make that employee one of the highest paid at the Department, earning more than agency leadership. These reservations, however,

similarly apply to other U.S. agencies who have nonetheless implemented new, enhanced recruitment incentives in recent years.

The competitive market for capable cyber personnel warrants the Department developing a hiring and retention strategy to ensure that it can attract a best-in-class cyber workforce to fulfill its investigative, prosecutorial, policy, and defensive responsibilities across dynamic present and future cyber threat environment. The Department should initiate an internal campaign to educate managers and budgetary personnel regarding existing hiring and retention incentives. This campaign should begin with clear policy guidance directing component leadership to: (1) prioritize their familiarization with such incentives; (2) submit proposals for applying such incentives to their cyber-related workforce; and (3) factor such incentives into future personnel projections. Such guidance should emphasize that fairness and perception concerns are not valid reasons to restrain the Department's recruitment and retention potential in the face of growing and evolving cyber threats. Over a longer term, the Department should establish a cross-component working group to explore collaboration with Congress to create new types of Federal civil service positions for the Department's cyber-related workforce.

> *"We need to develop the next generation of prosecutors with the training and experience necessary to combat the next generation of cyber threats."*
>
> DAG Lisa O. Monaco, Press Release Announcing Creation of New Cyber Fellows Program (Aug. 27, 2021)

In addition to more competitive incentives and salaries, the Department's cyber workforce strategy should implement novel means of attracting talent—including by offering junior hires opportunities to disrupt cyber threats in ways that are unique to the federal government and certainly unavailable outside the government. For example, in August 2021, following an interim recommendation from this review, the Deputy Attorney General announced the creation of the Department's new Cyber Fellows Program. This program will initially be available to new attorneys, but will expand to experienced attorneys with preexisting cyber-related talent. It will offer them the opportunity to develop as prosecutors across various offices that specialize in cyber investigations and prosecutions, including the CRM's CCIPS, CES, and the U.S. Attorney's Offices, many of which have specialized prosecutors. Upon the successful completion of their fellowship, these attorneys can choose a cyber-focused component for permanent employment.

Cyber Fellowship Program

In August 2021, Deputy Attorney General Lisa Monaco announced the creation of a new Cyber Fellowship program, designed to develop a new generation of prosecutors and attorneys equipped to handle emerging cybercrime and cyber-enabled national security threats.

The creation of the Fellowship is being coordinated through CCIPS. The three-year Cyber Fellowship will provide selected attorneys experience combating emerging national security and criminal cyber threats, while rotating through multiple department components that protect the nation from cyber threats — including CRM, NSD, and the U.S. Attorneys' Offices. Through this unique opportunity, Fellows will handle a broad range of the cyber cases handled by the Department and gain a comprehensive understanding of the Department's response to emerging and critical threats. Fellows can expect to investigate and prosecute state-sponsored cyber threats; transnational criminal groups; infrastructure and ransomware attacks; and the use of cryptocurrency and money laundering to finance and profit from cyber-based crimes.

The first class of Cyber Fellows is in the process of being finalized and will begin in the fall of 2022, concurrent with the incoming attorneys hired through the Department of Justice's Honors Program.

Appendix A: Notable DOJ Cybercrime Actions (2021)

2021.01.07 Russian national Andrei Tyurin sentenced to 144 months' imprisonment for role in hacking U.S. financial institutions, brokerage firms, and other U.S. victims.

2021.01.21 Conviction of Russian national Kirill Firsov for running DEER.IO platform that sold stolen personal information and credit cards. Firsov was later sentenced to 30 months' imprisonment.

2021.01.25 Conviction of Cypriot national Joshua Epifaniou for digital extortion of U.S. media companies and other victims.

2021.01.28 Disruption of Emotet botnet in coordinated cyber operation.

2021.02.17 Unsealed indictment of 3 North Korean Hackers for their role in WannaCry Ransomware attack, the disruptive attack on Sony Pictures Entertainment and cyber-enabled bank and cryptocurrency heists. Guilty plea of Canadian-American national Ghaleb Alaumary for role in money laundering for North Korean actors and others.

2021.03.18 Indictment of Swiss national Till Kottman for hacking more than 100 victim entities, particularly software developers, and FBI seizure of Kottman-operated website used to post stolen code.

2021.03.19 Russian national Sergey Medvedev and Macedonian national Marko Leopard sentenced to 10 years' and 5 years' imprisonment, respectively, for their role in hosting contraband merchants that caused more than $568 million in loss.

2021.04.12 Extradition of Arturs Zaharevics from the UK for his role in cybercriminal money laundering organization QQAAZZ.

2021.04.13 Court-authorized effort to disrupt exploitation of Microsoft Exchange Server vulnerabilities by actors associated with PRC intelligence services.

2021.05.07 Convictions of four Eastern European nationals for providing "bulletproof hosting" services to cybercriminals who attacked U.S. financial institutions and victims.

2021.06.01 Court-authorized seizure of domains used in furtherance of "Nobelium" spear-phishing campaign that posed as U.S. Agency for International Development.

2021.06.07 Court-authorized seizure of $2.3 million in bitcoin representing proceeds of DarkSide ransomware attack upon Colonial Pipeline.

2021.06.16 Conviction of Russian national Oleg Koshkin and Estonian national Pavel Tsurkan relating to crypting service Crypt4U, used to conceal malware such as the Kelihos botnet.

2021.06.28 Pavel Stassi sentenced to 24 months' imprisonment for "bulletproof hosting" of cybercriminals.

2021.07.19 Unsealed indictment of four nationals working with the PRC MSS for a hacking campaign targeting intellectual property and confidential business information, including infectious disease research.

2021.07.21 Arrest of UK national Joseph O'Connor a/k/a "PlugwalkJoe" in Spain pursuant to U.S. request, in connection with his hacking of social media accounts and cyberstalking. In August 2021, O'Connor was also indicted for "SIM swap attack" that resulted in theft of $784,000 in cryptocurrency.

2021.08.06 Convictions of Arturs Zaharevics and Aleksejs Trofimovics (2021.07.13) for their roles in the cybercriminal money laundering organization QQAAZZ.

2021.09.08 Ghaleb Alaumary sentenced to 140 months' imprisonment for money laundering related to a massive online banking theft by North Korean cyber criminals and other crimes.

2021.09.14 Three former U.S. Intelligence Community and military personnel entered into deferred prosecution agreements for developing zero-click exploits on behalf of UAE company, in violation of U.S. hacking and export control laws.

2021.09.16 Conviction of Matthew Gatrel for operation of hacking-for-hire downthem.org and ampnode.org that facilitated DDoS attacks.

2021.09.29 Indictment of Turkish national Mert Ozek Izzet for alleged use of WireX botnet to orchestrate DDoS attack on U.S. company.

2021.10.15 Conviction of hacker-for-hire Hao Kuo Chi a/k/a "icloudripper4you" for hacking into hundreds of iCloud accounts.

2021.10.20 Aleksandr Skorodumov sentenced to 48 months' imprisonment for "bulletproof hosting" of cybercriminals.

2021.10.20 Extradition of Russian national Vladimir Dunaev from South Korea for role in cybercriminal organization that deployed malware "Trickbot."

2021.11.05 Conviction of Chinese Intelligence Officer, Yanjun Xu, for conspiring to and attempting to commit economic espionage and theft of trade secrets.

2021.11.08 Arrest and announcement of charges against Yaroslav Vasinskyi, Ukrainian national allegedly responsible for Sodinokibi/REvil ransomware attack against Kaseya, and charges against and seizure of $6.1 million worth of bitcoin representing ransomware proceeds from Yevgeniy Polyanin, a Russian Sodinokibi/REvil actor.

2021.11.10 Russian Cybercriminal Aleksandr Zhukov sentenced to 10 years' imprisonment for "Methbot" fraud scheme targeting U.S. publishers and advertisers.

2021.11.18 Indictment of two Iranian nationals Seyyed Mohammad Hosein Musa Kazemi and Sajjad Kashian for their roles in cyber-enabled disinformation and threat campaign designed to influence the 2020 U.S. presidential election.

2021.12.01 Aleksandr Grichishkin sentenced to 60 months' imprisonment for "bulletproof hosting" of cybercriminals, including malware strains Zeus, SpyEye, Citadel, and the Blackhole Exploit Kit.

2021.12.07 Unsealing of indictment against Canadian Matthew Philbert, whom Canadian authorities described as "the most prolific cybercriminal we've identified in Canada."

2021.12.20 Extradition of Vladislav Klyushin from Switzerland for alleged role in hacking and illegal trading scheme.

---

[i] Deputy Attorney General Lisa Monaco, Memorandum for Heads of Department Components, "Comprehensive Cyber Review" (May 19, 2021).

[ii] *See* Dep't of Justice, Office of Public Affairs, "Ukrainian Arrested and Charged with Ransomware Attack on Kaseya," Nov. 8, 2021, *available at* https://www.justice.gov/opa/pr/ukrainian-arrested-and-charged-ransomware-attack-kaseya.

[iii] *See* Memorandum from Deputy Attorney General Lisa O. Monaco, "Guidance Regarding Investigations and Cases Related to Ransomware and Digital Extortion," June 3, 2021.

[iv] *Id*. at 1.

[v] *Id*. at 2. The reporting requirements applied to all investigations involving ransomware and/or digital extortion, as well as a subject or target under investigation primarily for the unlawful operation of such infrastructure frequently used in ransomware and digital extortion schemes, such as counter antivirus services, bulletproof hosting services, and cryptocurrency mixers.

[vi] Such tactics have been safely and successfully executed by the Department in the cyber domain since at least the 2011 disruption of the Coreflood botnet, in which the Department of Justice and the FBI used a variety of authorities, including a civil complaint, criminal seizure warrants, and a temporary restraining order, as part of a comprehensive enforcement action to disable an international botnet. See Dep't of Justice, Office of Public Affairs, "Department of Justice Takes Action to Disable International Botnet," April 13, 2011, available at https://www.justice.gov/opa/pr/department-justice-takes-action-disable-international-botnet.

[vii] *See* Dep't of Justice, Office of Public Affairs, "Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists DarkSide," June 7, 2021, *available at* https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside.

[viii] *See* Dep't of Justice, Office of Public Affairs, "Department of Justice Announces Court-Authorized Effort to Disrupt Exploitation of Microsoft Exchange Server Vulnerabilities," Apr. 13, 2021, *available at* https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-effort-disrupt-exploitation-microsoft-exchange.

[x] *See* Dep't of Justice, Office of Public Affairs, "Department of Justice Announces Court-Authorized Seizure of Domain Names Used in Furtherance of Spear-Phishing Campaign Posing as the U.S. Agency for International Development," June. 1, 2021, https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-seizure-domain-names-used-furtherance-spear. The seizure was accompanied by FBI and CISA's public release of a joint Cybersecurity Advisory regarding the campaign. CISA and FBI, Alert (AA21-148A), "Sophisticated Spearphishing Campaign Targets Government Organizations, IGOs, and NGOs," May 28, 2021, *available a*t https://www.cisa.gov/uscert/ncas/alerts/aa21-148a.

[xi] As with all techniques, the Department must conduct cyber operations appropriately and lawfully. Department lawyers should continue to carefully evaluate every operation to ensure that they fall within all legal limitations, especially the traditional protections of the United States Constitution. Additionally, Department lawyers should fully understand all risks posed by an operation, not only to the investigation, but also to any potential innocent third parties. As the Assistant Attorney General for the Criminal Division previously wrote:

> As with law enforcement activities in the physical world, law enforcement actions to prevent or redress online crime can never be completely free of the risk of unintended consequences. For this reason, before we conduct online investigations, the Department of Justice carefully considers both the public safety needs and the potential risks. In particular, when conducting complex online operations, we strive to work closely with sophisticated computer security researchers both inside and outside the government. As part of operational mission planning, investigators conduct pre-deployment verification and validation of computer tools. Such testing is designed to ensure that tools work as intended and do not create unintended consequences. That kind of careful consideration of any future technical measures will continue.

See Assistant Attorney General Leslie R. Caldwell, Criminal Division, "Additional Considerations Regarding the Proposed Amendments to the Federal Rules of Criminal Procedure," Nov. 28, 2016, *available at* https://www.justice.gov/archives/opa/blog/additional-considerations-regarding-proposed-amendments-federal-rules-criminal-procedure.

[xii] *See* Dep't of Justice, Office of Public Affairs, "Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe," Feb. 17, 2021, *available at* https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and.

[xiii] See, e.g., Dep't of Justice, Office of Public Affairs, "Remarks by Deputy Attorney General Jeffrey A. Rosen at the Announcement of Charges and Arrests in Relation to Computer Intrusion Campaigns Related to China," Sept. 16, 2020, *available at* https://www.justice.gov/opa/speech/remarks-deputy-attorney-general-jeffrey-rosen-announcement-charges-and-arrests-computer; Dep't of Justice, Office of Public Affairs, "Two Chinese Hackers Working With the Ministry of State Security Charged With Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Covid-19 Research," July 21, 2020, available at https://www.justice.gov/usao-edwa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion; Dep't of Justice, Office of Public Affairs, "U.S. Charges Russian FSB Officers and Their Criminal Conspirators for Hacking Yahoo and Millions of Email Accounts," Mar. 15, 2017, *available at* https://www.justice.gov/opa/pr/us-charges-russian-fsb-officers-and-their-criminal-conspirators-hacking-yahoo-and-millions.

[xiv] Microsoft, "New Nation-State Cyberattacks," Mar. 2, 2021, *available at* https://blogs.microsoft.com/on-the-issues/2021/03/02/new-nation-state-cyberattacks/. The U.S. Government and allies subsequently attributed early aspects of this malicious activity to the People's Republic of China. *See* White House Briefing Room, "The United States, Joined by Allies and Partners, Attributes Malicious Cyber Activity and Irresponsible State Behavior to the People's Republic of

China," July 19, 2021, *available at* https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/19/the-united-states-joined-by-allies-and-partners-attributes-malicious-cyber-activity-and-irresponsible-state-behavior-to-the-peoples-republic-of-china/.

[xv] *See* Memorandum from Deputy Attorney General Jeffrey A. Rosen, "Policy, Procedures, and Guidance Regarding Discoverable Information in Criminal Investigations Possessed by the Intelligence Community or Military," Sept. 11, 2020.

[xvi] *See* Dep't of Justice, Office of Public Affairs, "North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions," Sept. 6, 2018, *available at* https://www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and.

[xvii] *See* Dep't of Justice, Office of Public Affairs, "Three North Korean Military Hackers Indicted in Wide-Ranging Scheme to Commit Cyberattacks and Financial Crimes Across the Globe," Feb. 17, 2021, *available at* https://www.justice.gov/opa/pr/three-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and.

[xviii] *See* Dep't of Justice, Office of Public Affairs, "International Money Launderer Sentenced to Over 11 Years in Federal Prison for Laundering Millions from Cyber Crime Schemes," Sept. 8, 2021, *available at* www.justice.gov/usao-cdca/pr/international-money-launderer-sentenced-over-11-years-federal-prison-laundering

[xix] *See* Dep't of Justice, Office of Public Affairs, "Four Individuals Plead Guilty to RICO Conspiracy Involving "Bulletproof Hosting" for Cybercriminals," May 7, 2021, *available at* https://www.justice.gov/opa/pr/four-individuals-plead-guilty-rico-conspiracy-involving-bulletproof-hosting-cybercriminals.

[xx] *See* Dep't of Justice, Office of Public Affairs, "Ohio Resident Pleads Guilty to Operating Darknet-Based Bitcoin 'Mixer' That Laundered Over $300 Million," Aug. 18, 2021, *available at* https://www.justice.gov/opa/pr/ohio-resident-pleads-guilty-operating-darknet-based-bitcoin-mixer-laundered-over-300-million.

[xxi] *See* Dep't of Justice, Office of Public Affairs," Russian National Convicted of Charges Relating to Kelihos Botnet," June 16, 2021, *available at* https://www.justice.gov/usao-ct/pr/russian-national-convicted-charges-relating-kelihos-botnet.

[xxii] *See* Europol, "Unhappy New Year for Cybercriminals as VPNLab.net Goes Offline," Feb. 1, 2022, *available at* https://www.europol.europa.eu/media-press/newsroom/news/unhappy-new-year-for-cybercriminals-vpnlabnet-goes-offline.

[xxiii] *See* Dep't of Justice, Office of Public Affairs, "Seven International Cyber Defendants, Including "APT41 Actors Charged in Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally," Sept. 16, 2020, *available at* https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer.

[xxiv] *See* Dep't of Justice, Office of Public Affairs, "Two Arrested for Alleged Conspiracy to Launder $4.5 Billion in Stolen Cryptocurrency," Feb. 8, 2022, *available at* https://www.justice.gov/opa/pr/two-arrested-alleged-conspiracy-launder-45-billion-stolen-cryptocurrency.

[xxv] *See* Dep't of Justice, Office of Public Affairs, "United States Seizes Domain Names Used by Iran's Islamic Revolutionary Guard Corps," Oct. 7, 2020, *available at* https://www.justice.gov/opa/pr/united-states-seizes-domain-names-used-iran-s-islamic-revolutionary-guard-corps; see also Dep't of Justice, Office of Public Affairs, "Chinese Military Personnel Charged with Computer Fraud, Economic Espionage, and Wire Fraud for Hacking into Credit Reporting Agency Equifax," Feb. 10, 2020, *available at* https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking.

[xxvi] *See* Dep't of Justice, Office of Public Affairs, "Justice Department Announces Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate (GRU)," Apr. 6, 2022, *available at* https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-disruption-botnet-controlled-russian-federation.

[xxvii] *See* Dep't of Justice, Office of Public Affairs, "Department of Justice Announces Actions to Disrupt Advanced Persistent Threat 28 Botnet of Infected Routers and Network Storage Devices," May 23, 2018, *available at* https://www.justice.gov/opa/pr/justice-department-announces-actions-disrupt-advanced-persistent-threat-28-botnet-infected.

[xxviii] *See* Dep't of Justice, Office of Public Affairs, "Six Russian GRU Officers Charged in Connection with Worldwide Deployment of Destructive Malware and Other Disruptive Actions in Cyberspace," Oct. 19, 2020, *available at* https://www.justice.gov/opa/pr/six-russian-gru-officers-charged-connection-worldwide-deployment-destructive-malware-and.

[xxix] *See Federal Sentencing of Child Pornography: Production Offenses*, United States Sentencing Commission (Oct 2021), at 17, *available at* https://www.ussc.gov/sites/default/files/pdf/research-and-publications/research-publications/2021/20211013_Production-CP.pdf.

[xxx] *See* Dep't of Justice, Office of Public Affairs, "Two Iranian Nationals Charged for Cyber-Enabled Disinformation and Threat Campaign Designed to Influence the 2020 U.S. Presidential Election," Nov. 18, 2021, *available at* https://www.justice.gov/opa/pr/two-iranian-nationals-charged-cyber-enabled-disinformation-and-threat-campaign-designed.

[xxxi] *See* Dep't of Justice, Office of Public Affairs, "U.S. Charges Russian GRU Officers with International Hacking and Related Influence and Disinformation Operations," Oct. 4, 2018, *available at* https://www.justice.gov/opa/pr/us-charges-russian-gru-officers-international-hacking-and-related-influence-and.

[xxxii] *See* Report of the Attorney General's Cyber Digital Task Force, July 2, 2018, Chapter 1, *available at* https://www.justice.gov/archives/ag/page/file/1076696/download.

[xxxiii] *See* Executive Assistant Director Jill Sanborn, "The Domestic Terrorism Threat One Year After January 6," Testimony Before the Senate Judiciary Committee," Jan. 11, 2022, *available at* https://www.fbi.gov/news/testimony/the-domestic-terrorism-threat-one-year-after-january-6-011122.

[xxxiv] Assistant Attorney General Matthew G. Olsen, Remarks Before U.S. Senate Committee on the Judiciary, Jan. 11, 2022, *available at* https://www.justice.gov/opa/speech/assistant-attorney-general-matthew-g-olsen-delivers-opening-remarks-us-senate-committee.

[xxxv] *See* Executive Assistant Director Jill Sanborn, "The Domestic Terrorism Threat One Year After January 6," Testimony Before the Senate Judiciary Committee," Jan. 11, 2022, *available at* https://www.fbi.gov/news/testimony/the-domestic-terrorism-threat-one-year-after-january-6-011122.

[xxxvi] *See* White House, National Strategy for Countering Domestic Terrorism, June 2021, *available at* https://www.whitehouse.gov/wp-content/uploads/2021/06/National-Strategy-for-Countering-Domestic-Terrorism.pdf.

[xxxvii] *See* Assistant Director Timothy Langan, "Countering Domestic Terrorism," Nov. 3, 2021, *available at* https://www.fbi.gov/news/testimony/countering-domestic-terrorism-110321.

[xxxviii] For example, in June 2021 the Department announced convictions of U.S. and Canadian nationals who were self-described members of "The Base," a coalition of white supremacist members within the United States and abroad built through, among other things, online chat rooms. Dep't of Justice, Office of Public Affairs, "Two Members of the Violent Extremist Group 'The Base' Plead Guilty to Federal Firearms and Alien-Related Charges," June 10, 2021, *available at* https://www.justice.gov/usao-md/pr/two-members-violent-extremist-group-base-plead-guilty-federal-firearms-and-alien-related. In March 2021, the Intelligence Community assessed that U.S. racially or ethnically motivated violent extremists who promote the superiority of the white race are the DVE actors with the most persistent and concerning transnational connections because individuals with similar ideological beliefs exist outside of the United States and these RMVEs frequently communicate with and seek to influence each other. *See* Office of the Director of National Intelligence, "Domestic Violent Extremism Poses Heightened Threat in 2021," Mar. 1, 2021, *available at* https://www.dni.gov/files/ODNI/documents/assessments/UnclassSummaryofDVEAssessment-17MAR21.pdf.

[xxxix] *See*, e.g., Dep't of Justice, "Department of Justice Participates Virtually at G7 Meeting with Security Ministers," https://www.justice.gov/opa/pr/justice-department-participates-virtually-g7-meeting-security-ministers; "G7 London Interior Commitments," G7 Interior and Security Ministers' Meeting, Sept. 2021, *available at* https://www.gov.uk/government/publications/g7-interior-and-security-ministers-meeting-september-2021/g7-london-interior-commitments-accessible-version; Dep't of Justice, Office of Public Affairs, "Attorney General Garland Participates in Quintet Meeting of Attorneys General," Dec. 9, 2021, *available at* https://www.justice.gov/opa/pr/attorney-general-garland-participates-quintet-meeting-attorneys-general; Dep't of Justice, Office of Public Affairs, Virtual Quintet of Attorneys-General Communiqué, Dec. 2-3, 2021, *available at* https://www.justice.gov/opa/press-release/file/1454381/download; Dep't of Justice, Office of Public Affairs, "Joint U.S.-EU statement following the U.S.-EU Justice and Home Affairs Ministerial," Dec. 17, 2021, *available at* https://www.justice.gov/opa/pr/joint-us-eu-statement-following-us-eu-justice-and-home-affairs-ministerial; Dep't of Justice, Joint U.S.-EU statement following the U.S.-EU Justice and Home Affairs Ministerial Meeting, Washington, D.C., Dec. 16, 2021, *available at* https://www.justice.gov/opa/press-release/file/1457246/download.

[xl] *See* White House, National Strategy for Countering Domestic Terrorism, June 2021, *available at* https://www.whitehouse.gov/wp-content/uploads/2021/06/National-Strategy-for-Countering-Domestic-Terrorism.pdf.

[xli] OFAC is authorized to sanction a variety of cyber actors pursuant to existent authorities, most notably Executive Order (E.O.) 13694 ("Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities"), as amended by E.O. 13757 ("Taking Additional Steps to Address the National Emergency With Respect to Significant Malicious Cyber-Enabled Activities"). Other operative executive orders include Executive Order 13581 ("Blocking Property of Transnational Criminal Organizations") and Executive Order 13687 ("Imposing Additional Sanctions with Respect to North Korea").

[xlii] TORCP was established by Congress in 2013 as a tool to assist the U.S. Government to identify and bring the justice members of significant transnational criminal organizations. The program gives the Secretary of State statutory authority to offer rewards for information leading to the arrest and/or conviction of members of transnational criminal organizations who operate outside the United States. The Department of State's Bureau of International Narcotics and Law Enforcement Affairs manages the program in close coordination with U.S. federal law enforcement agencies. The State Department has issued multiple reward offers of up to $10,000,000 for information about specific ransomware groups.

[xliii] RFJ was established by the 1984 Act to Combat International Terrorism, Public Law 98-533 (codified at 22 U.S.C. § 2708). Under this program, the Secretary of State may authorize rewards for information that leads to the arrest or conviction of anyone who plans, commits, aids, or attempts international terrorist acts against U.S. persons or property; that prevents such acts from occurring in the first place; that leads to the identification or location of a key terrorist leader; or that disrupts terrorism financing. In recent years, the State Department has announced rewards for cyber-related activity, including a reward of up to $10 million related to any person who, while acting at the direction or under the control of a foreign government, targets U.S. critical infrastructure through unlawful computer intrusions. *See* State Department, "Foreign Malicious Cyber Activity Against U.S. Critical Infrastructure," *available at* https://rewardsforjustice.net/english/malicious_cyber_activity.html.

[xliv] *See* Dep't of Justice, Office of Public Affairs, "Two Iranian Nationals Charged for Cyber-Enabled Disinformation and Threat Campaign Designed to Influence the 2020 U.S. Presidential Election," Nov. 18, 2021, *available at* https://www.justice.gov/opa/pr/two-iranian-nationals-charged-cyber-enabled-disinformation-and-threat-campaign-designed.

[xlv] *See* U.S. Dep't of State, Office of the Spokesperson, "Rewards for Justice – Reward Offer for Information on Iranian Cyber Actors' Interference with 2020 U.S. Presidential Election," Feb. 1, 2022, *available at* https://www.state.gov/rewards-for-justice-reward-offer-for-information-on-iranian-cyber-actors-interference-with-2020-u-s-presidential-election/.

[xlvi] *See* Dep't of Justice, Office of Public Affairs, "Two Chinese Nationals Charged with Laundering Over $100 Million in Cryptocurrency from Exchange Hack," Mar. 2, 2020, *available at* https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack.

[xlvii] *See* Dep't of Justice, Office of Public Affairs, "United States Files Complaint to Forfeit 280 Cryptocurrency Accounts Tied to Hacks of Two Exchanges by North Korean Actors," Aug. 27, 2020, *available at* https://www.justice.gov/opa/pr/united-states-files-complaint-forfeit-280-cryptocurrency-accounts-tied-hacks-two-exchanges.

[xlviii] Presidential Policy Directive-41, "United States Cyber Incident Coordination," July 26, 2016, *available at* https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident ("In view of the fact that significant cyber incidents will often involve at least the possibility of a nation-state actor or have some other national security nexus, the Department of Justice, acting through the Federal Bureau of Investigation and the National Cyber Investigative Joint Task Force, shall be the Federal lead agency for threat response activities.").

[xlix] Today, IOD has 63 Legat offices and 30 sub-offices in key cities around the globe, providing coverage for more than 180 countries, territories, and islands. Nearly all of those offices work with local partners against cyber threats, while FBI's 16 Cyber Assistant Legal Attachés (ALATs), all technically-trained agents, often embed with law enforcement and intelligence counterparts to maximize joint operational planning and information exchange.

[l] The GLEN program is the result of a partnership between the Department of State's Bureau of International Narcotics and Law Enforcement Affairs (INL) and the Department of Justice's CCIPS and OPDAT. The GLEN relies in part on Department attorneys serving as ICHIP coordinators. Currently, ICHIPs are posted in countries across five different continents. *See* Dep't of Justice, Criminal Division, "Global Cyber and Intellectual Property Crimes," *available at* https://www.justice.gov/criminal-opdat/global-cyber-and-intellectual-property-crimes.

[li] *See* Dep't of Justice, Office of Public Affairs, "Russian National Extradited to United States to Face Charges for Alleged Role in Cybercriminal Organization," Oct. 28, 2021, *available at* https://www.justice.gov/opa/pr/russian-national-extradited-united-states-face-charges-alleged-role-cybercriminal.

[lii] *See* Dep't of Justice, Office of Public Affairs, "Jury Convicts Chinese Intelligence Officer of Espionage Crimes, Attempting to Steal Trade Secrets," Nov. 5, 2021, *available at* https://www.justice.gov/opa/pr/jury-convicts-chinese-intelligence-officer-espionage-crimes-attempting-steal-trade-secrets.

[liii] *See* Dep't of Justice, Office of Public Affairs, "Russian National Extradited for Role in Hacking and Illegal Trading Scheme," Dec. 20, 2021, *available at* https://www.justice.gov/usao-ma/pr/russian-national-extradited-role-hacking-and-illegal-trading-scheme.

[liv] In 2019, for example, the EU established a framework for a joint diplomatic response to malicious cyber activities, called the "Cyber Diplomacy Toolbox." The measures consist of asset freezes and travel bans for persons and entities responsible for cyberattacks, as well as those involved in or offering financial, technical, or material support for these attacks and those who assist, encourage, facilitate, or are associated with them. Since then, the EU has implemented three rounds of cyber sanctions against Chinese, Russian, and North Korean actors and entities, in July, October, and November 2020. Notably, each of these designations came after the Department obtained public criminal charges related to the same malicious cyber activities. These types of actions make clear that the reach of the collective ability of the U.S. Government and its partners to hold individuals and entities accountable no matter their location. See EU Sanctions Map, Cyber-Attacks, *available at* https://www.sanctionsmap.eu/#/main/details/47/?search=%7B%22value%22:%22%22,%22searchType%22:%7B%7D%7D (last visited Jan. 28, 2022).

[lv] *See* Dep't of State, "Rewards Offers for Information to Bring Sodinokibi (REvil) Ransomware Variant Co-Conspirators to Justice, Nov. 8, 2021, *available at* https://www.state.gov/reward-offers-for-information-to-bring-sodinokibi-revil-ransomware-variant-co-conspirators-to-justice/

[lvi] *See* Europol, "Five Affiliates to Sodinokibi/REvil Unplugged," Nov. 8, 2021, *available at* https://www.europol.europa.eu/media-press/newsroom/news/five-affiliates-to-sodinokibi/revil-unplugged

[lvii] *See* Council of Europe, "Protocol Negotiations," *available at* https://www.coe.int/en/web/cybercrime/t-cy-drafting-group. The Protocol is expected to be open for signature in May 2022. *Id*.

[lviii] *See* Dep't of Justice, White Paper, "Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act," Apr. 2019, *available at* https://www.justice.gov/opa/press-release/file/1153446/download.

[lix] White House Briefing Room, "Joint Statement on the Visit to the United Kingdom of the Honorable Joseph R. Biden, Jr., President of the United States of America at the Invitation of the Rt. Hon. Boris Johnson, M.P., the Prime Minister of the United Kingdom of Great Britain and Northern Ireland," June 10, 2021, *available at* https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/10/joint-statement-on-the-visit-to-the-united-kingdom-of-the-honorable-joseph-r-biden-jr-president-of-the-united-states-of-america-at-the-invitation-of-the-rt-hon-boris-johnson-m-p-the-prime-min/.

[lx] FBI Director Wray, Keynote Address, CISA Cyber Security Summit (Sept. 16, 2020), *available at* https://www.fbi.gov/video-repository/wray-cisa-091620.mp4/view.

[lxi] National Center for Missing and Exploited Children, "2020 Reports by Electronic Service Providers (ESP)," *available at* https://www.missingkids.org/content/dam/missingkids/gethelp/2020-reports-by-esp.pdf.

[lxii] *See, e.g.*, Dep't of Justice, "Best Practices for Victim Response and Reporting of Cyber Incidents," Sept. 2018, *available at* https://www.justice.gov/criminal-ccips/file/1096971/download.

[lxiii] *See* Assistant Director Scott S. Smith, Statement Before the Senate Armed Services Committee, "Roles and Responsibilities for Defending the Nation from Cyber Attack," Oct. 19, 2017, *available at* https://www.fbi.gov/news/testimony/cyber-roles-and-responsibilities.

[lxiv] *See, e.g.*, Cybersecurity & Infrastructure Security Agency, "CISA, FBI, and NSA Release Cybersecurity Advisory on Russian Cyber Threats to U.S. Critical Infrastructure," Jan. 11, 2022, *available at* https://www.cisa.gov/uscert/ncas/current-activity/2022/01/11/cisa-fbi-and-nsa-release-cybersecurity-advisory-russian-cyber; Cybersecurity & Infrastructure Security Agency, "CISA, FBI, and NSA Release Joint Cybersecurity Advisory on Conti Ransomware," Sept. 22, 2021, *available at* https://www.cisa.gov/uscert/ncas/current-activity/2021/09/22/cisa-fbi-and-nsa-release-joint-cybersecurity-advisory-conti.

[lxv] The IC3 received 847,376 complaints filed direct through its website, reporting total losses of $20.9 billion. The IC3 also receives an additional 112,208 complaints reporting $37.3 million in losses. These additional complaints are ingested into the IC3 database directly from the National Center for Disaster Fraud, Federal Trade Commission, and the FBI National Threat Operation Center.

[lxvi] The IC3 RAT was established in February 2018 to streamline communication with financial institutions and assist FBI field offices with the freezing of funds for victims who made transfers to domestic accounts under fraudulent pretenses.

[lxvii] Created by the FBI, the FFKC is a process for recovering large international wire transfers stolen from U.S. victim bank accounts.

[lxviii] For example, the report found that over 100,000 persons over the age of 60 filed a complaint, with a resulting loss of nearly $1 billion, although the greatest financial losses were associated with confidence fraud/romance scams. For elder fraud, victims have the choice of reporting fraud to the Department either through the IC3 portal or by calling the National Elder Fraud Hotline, 1-833-FRAUD-11 (1-833-372-8311).

[lxix] E.O. 14028, "Executive Order on Improving the Nation's Cybersecurity," May 12, 2021, *available at* https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[lxx] The term "Zero Trust Architecture" refers to a security model, a set of system design principles, and a coordinated cybersecurity and system management strategy based on an acknowledgement that threats exist both inside and outside traditional network boundaries. The Zero Trust security model eliminates implicit trust in any one element, node, or service and instead requires continuous verification of the operational picture via real-time information from multiple sources to determine access and other system responses. Older models of security essentially focus on building a digital wall around

systems and keeping actors outside those walls; if a malicious actor gains makes it past those walls, however, the systems are relatively unprotected. Zero Trust Architecture, in turn, focuses on building a system of constant checks inside the network, assuming that not everyone inside the proverbial walls can be trusted.

[lxxi] The most notable form of code-based compromise is through social engineering—for example, when a user is deceived by the adversary into disclosing the randomly generated number under the guise of IT support or a security verification process. PIV cards are not similarly susceptible.

[lxxii] An exception to multi-factor authentication might be granted under existing Department policies, for example, if an employee forgets his or her PIV card at home or encounters a technical difficulty with the multi-factor process for a system.

[lxxiii] Office of Management and Budget, M-21-31 "Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents" (Aug. 27, 2021).

[lxxiv] Principal Associate Deputy Attorney General Richard O. Donoghue, Memorandum, "Electronic Filing of Highly Sensitive Materials," January 8, 2021.

[lxxv] During its assessment of the SolarWinds compromise, OCIO concluded that certain safeguards intended to better segment email on the vendor's system—making it harder for a wholesale exfiltration of data—did not operate as intended. The failure exacerbated the total loss of data during the December 2020 intrusion.

[lxxvi] 31 U.S.C. § 3729 et seq.

[lxxvii] JM 9-95.000. The UAS Policy permits the use of UAS only in connection with properly authorized investigations and activities. It also requires compliance with the Constitution and all applicable laws and regulations, including regulations issued by the Federal Aviation Administration.

[lxxviii] It is Department policy that an IPA should be completed as early as possible during the design and development of, or any significant modification to, a project in which the Department knows it will, or is unsure whether it will, create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable information.

[lxxxix] *See* Dep't of Defense, "DoD Excepted Service (CES) Personnel System," Aug. 2017, *available at* https://dl.dod.cyber.mil/wp-content/uploads/dces/pdf/CESOverviewFactSheet.pdf.

[lxxx] *See, e.g.*, Cybersecurity Talent Management System, 86 Fed. Reg. 47,840 (Aug. 26, 2021) (DHS interim final rule)

[lxxxi] *See, e.g.*, USAJobs, Announcement DE-11354787-22-YMF, "Chief Counsel for Cybersecurity and Infrastructure Security Agency," *available at* https://www.usajobs.gov/job/631415300.

[lxxxii] 5 U.S.C 5305 and 5 CFR part 530, subpart C.

[lxxxiii] *See, e.g.*, 5 CFR 451.104(a)(1) & (2) (setting forth awards).

[lxxxiv] 5 U.S.C. 5753 and 5 CFR part 575, subpart A.

[lxxxv] 5 CFR 531.212.

[lxxxvi] *See* 5 U.S.C. § 3131 (establishing Senior Executive Service)