

## 2. Enduring Partnerships

The FBI has several established programs that enable connectivity, information sharing, and collaboration with the private sector on a range of hazards, including cyber threats. These programs include:



**Domestic Security Alliance Council** (“DSAC”) was founded in 2006 as a national membership program to encourage public-private engagement between corporate chief security officers and the FBI on emerging threats facing the nation and economy. DHS was later added as a partner organization. With over 500 member companies, DSAC provides the FBI and DHS direct engagement with decision-makers in the U.S. economy’s largest corporations and critical insight through the DSAC Executive Working Group.



**InfraGard** is a partnership between the FBI and members of the private sector for sharing information and promoting mutual learning

relevant to the protection of the nation’s critical infrastructure. In contrast to DSAC, InfraGard members join as individuals, not as corporations. There are over 50,000 vetted InfraGard members nationally, representing all critical infrastructure sectors, organized into 84 local chapters called “InfraGard Member Alliances.” Each chapter is associated with its corresponding local FBI field office.



**National Cyber-Forensics & Training Alliance** (“NCFTA”) was conceived in 1997 and the non-profit 501(c)(3) corporation was created in 2003. Headquartered in Pittsburgh, this organization has become an international model for joining law enforcement, private industry, and academia to build and share resources, strategic information, and cyber threat intelligence. Since its establishment, the NCFTA has evolved to keep up with the ever-changing cybercrime landscape. Today, the organization deals with threats from transnational criminal groups including spam, botnets, stock manipulation schemes, intellectual property theft, pharmaceutical fraud, telecommunication scams, and other financial fraud schemes that result in billions of dollars in losses to companies and consumers. The extensive knowledge base within the NCFTA has played a key role in some of the FBI’s most significant cyber cases in the past several years.



**National Domestic Communications Assistance Center** (“NDCAC”) is a national hub for technical knowledge management among law enforcement agencies that also strengthens law enforcement’s relationships with the communications industry. Operated by the FBI’s Operational Technology Division, the NDCAC leverages and shares law enforcement’s collective technical knowledge and resources on issues involving real-time and stored communications to address challenges posed by advanced communications services and technologies. NDCAC develops and maintains relationships with industry to ensure law enforcement’s understanding of new services and technologies, and it provides a venue to exchange information, streamline processes, and facilitate more efficient interaction between law enforcement and industry. NDCAC also educates industry on law enforcement’s evidentiary processes and works with industry to verify that technical solutions work as expected.



**Internet Crime Complaint Center** (“IC3”) provides the public with a reliable and convenient reporting mechanism to submit information to the FBI concerning suspected

Internet-facilitated criminal activity and to develop effective alliances with law enforcement and industry partners. Since 2000, the IC3 has received complaints crossing the spectrum of cybercrime matters, to include online fraud in its many forms, including Intellectual Property Rights (“IPR”) matters, computer intrusions, economic espionage, online extortion, identity theft and others. It is through this reporting that the program is able to analyze complaints for dissemination to the public, private industry, and for intelligence/investigative purposes for law enforcement.

### ***3. Reporting Cyber Incidents and Notifying Targeted Entities***

Through the numerous FBI and U.S. Attorneys’ offices nationwide, the Department is uniquely positioned to interact with organizations that have experienced a cyber incident. The FBI has 56 field offices throughout the country, and has assisted victims of crime for over 100 years, including since the earliest days of computer crime. The FBI may learn through law enforcement or intelligence sources that a U.S. person or organization has suffered an incident or is the target of illicit cyber activity, and can proactively notify the targeted entity. Conversely, victims may be the first to detect the incident and then can notify the FBI. In either case, the Department stands ready to investigate the unauthorized activity and support victims.

#### ***Victim Notification***

The Department identifies victims of cyber intrusion through a variety of means, such

as from the FBI's ongoing contact with victims, from investigations of threat actors, from other members of the U.S. Intelligence Community, and from foreign partners. This information may be highly classified or may carry special handling or sharing restrictions based on the sensitivity of the source and the information provided. The FBI takes all reasonable steps to identify the targeted individual or entity, determine if there was an actual compromise, and assess if there is actionable information it may share.

Depending upon the circumstances, the FBI can undertake direct or indirect notice to victims or potential victims. "Direct" notification is typically handled in-person through established liaison contacts, such as by notifying the representatives of an institutional victim. Larger scale data breaches involving thousands or millions of affected customers are more complicated. In such circumstances, the FBI relies on victimized institutions to provide notification to affected individuals. In those cases, the victimized institution may be better situated to notify its customers or members of a large-scale data breach.

#### *Reporting Intrusions to the FBI*

While law enforcement and intelligence agencies can sometimes uncover malicious cyber activity before a victim detects it on their networks, in other cases a targeted organization will be the first to detect anomalous activity. It is critically important to report incidents to law enforcement, as each incident potentially involves the commission of a federal crime and may warrant investigation. The FBI is uniquely positioned to investigate and attri-

bute malicious cyber activity due to its dual criminal investigative and national security responsibilities.

While cyberattacks are typically conducted through technical means, behind the malicious activity is an actual individual or group perpetrating a crime. When the FBI is promptly notified, it can work to determine who caused the incident, link the incident to other incidents, maximize investigative opportunities, and potentially provide context regarding the actor, their tradecraft, and their motivations. Understanding who is targeting a victim's networks and for what purpose can inform defensive strategies and prevent future attacks. By notifying and assisting law enforcement, victims also help the FBI identify and pursue those responsible—which can help prevent future crimes against other victims. Such identification and pursuit is not limited to criminal response options. For example, attribution resulting from FBI investigative activities can support other U.S. government agencies' abilities to impose regulatory (e.g., sanctions), diplomatic, and technical costs upon those responsible for, or benefiting from, malicious cyber activities. Finally, notifying law enforcement may also place a victim company in a positive light with regulators, shareholders, and the public.

The Department encourages key organizations, particularly critical infrastructure owners and operators, to identify and form relationships with personnel in their local FBI field office, including through the partnerships detailed above, *before* an incident occurs. These pre-established relationships

and open lines of communication will speed reporting and response efforts.

The White House's Council of Economic Advisors recently observed that most data breaches are not reported to the U.S. government.<sup>2</sup> This reluctance may be driven by a fear of regulatory action, of reputational harm, or of an interruption to business operations. The reluctance of organizations and businesses to disclose that they have been attacked constitutes a major challenge for the U.S. government in its battle against cybercrime. Law enforcement cannot be effective without the cooperation of crime victims. A lack of cooperation may not only prevent discovery of evidence that could lead to identifying and holding the threat actors accountable, but also creates barriers to fully understanding the threat environment.

## Responding to Cyber Incidents and Managing Crisis

### 1. Policy Framework

Presidential Policy Directive ("PPD")-41, titled "United States Cyber Incident Coordination," defines the term "cyber incident,"<sup>3</sup> and describes cyber incident response in terms of three concurrent and mutually beneficial lines of effort: **threat response** (investigation, attribution, and threat pursuit); **asset response** (remediation and recovery); and **intelligence support**. It also refers to a fourth, unnamed line of effort that is best described as "**business response**" (ensuring business continuity, addressing legal and regulatory issues, and external affairs). In the context of

a nationally significant cyber incident, these activities are carried out in a coordinated way by the affected entity, by its third-party cybersecurity providers (if any), and by relevant federal agencies.

PPD-41 designates the Department of Justice, through the FBI and the National Cyber Investigative Joint Task Force ("NCIJTF"), as the lead federal agency for threat response activities in the context of a significant cyber incident. Through evidence collection, technical analysis, and related investigative tools, the FBI works to quickly identify the source of a cyber incident, connect that incident with related incidents, and determine attribution.

In addition to the cyber incident response framework laid out in PPD-41, the federal government also has adopted a Cyber Incident Severity Schema,<sup>4</sup> a rubric for describing an incident's significance and improving the federal government's response. An *incident of national significance* is rated as a Level 3 "High" (Orange), or greater. While the FBI does not allocate resources based exclusively on the schema rating, the rating serves as an enabler to various multi-agency coordination procedures and incident response efforts.

Both PPD-41 and the severity schema recognize that not all cyber incidents are "significant" from a national perspective. Thus, the scale and speed of a federal response will vary based on the facts and circumstances of particular cases. The FBI has capability, plans, and procedures to manage routine incidents. It also is prepared to react to circumstances



requiring a more robust approach. Responses to both types of incidents are discussed below.

## ***2. Routine Incident Response***

The FBI's nationwide reach puts it in an optimal position to engage with potential victims. The FBI's field-centric model also allows it to respond quickly, and in-person, to cyber incidents—often in a matter of hours.

Each FBI field office houses a multi-agency Cyber Task Force (“CTF”) modeled after the FBI's successful Joint Terrorism Task Force program. The task forces bring together cyber investigators, prosecutors, intelligence analysts, computer scientists, and digital forensic technicians from various federal, State, and local agencies present within the office's territory. The CTFs not only serve as a force multiplier, but also provide a forum for coordination amongst local partners for more effective incident response. This model also allows the FBI to draw on the relationships, expertise, authorities, and tools of the task force members.

In addition to these cyber-specific resources, the FBI has other technical assets it can use as needed to combat cyber threats. The FBI's Operational Technology Division develops and maintains a wide range of sophisticated equipment, capabilities, and tools to support investigations and to assist with technical operations. While every FBI field office has a computer forensics laboratory, certain field offices host a larger Regional Computer Forensic Laboratory. These resources can be leveraged throughout the FBI's response and investigative cycle to respond to cyber threats.

The FBI also has a strong international reach through a network of approximately 80 Legal Attaché offices throughout the world. It has supplemented 20 of these international offices with cyber-specific investigators to facilitate cooperation and information sharing to advance its cybercrime and national security investigations.

Because cyber threats and incidents occur around the clock, the FBI in 2014 established a steady-state, 24-hour watch capability called CyWatch. Housed at the NCIJTF, CyWatch is responsible for coordinating domestic law enforcement response to criminal and national security cyber intrusions, tracking victim notification, and partnering with the other federal cyber centers many times each day. CyWatch provides continuous connectivity to interagency partners to facilitate information sharing, and real-time incident management and tracking, as part of an effort to ensure that all relevant agencies are in communication.

## ***3. Significant Incident Response***

As directed by PPD-41, the FBI activates certain “enhanced coordination procedures” in the event of a “significant cyber incident.”<sup>5</sup> These procedures include naming an accountable senior executive to manage the response and establishing a dedicated command center with a full array of communication capabilities.

Members of the local FBI Cyber Task Force will respond to the significant incident and a designated special agent will serve as the U.S. government's point of contact to the victim throughout the response. Nearby FBI field

## Tips for Cooperative Cyber Incident Response

### Preparation

- Develop a response plan that incorporates **notifying and collaborating with law enforcement**.
- **Establish a relationship with your local FBI Cyber Task Force and U.S. Attorney's Office** in advance of an incident; invite them to participate in exercises.
- Understand the threats and trends that may affect your organization and adjust defenses accordingly; FBI and DHS regularly publish relevant reports.

### Discovery & Response

- **Notify the FBI\* when you experience an incident**; your issue may be part of a larger adversary campaign.
- **Preserve key evidence** that will enable investigators to attribute the incident and pursue the actors (e.g., logs and artifacts, affected devices, analysis reports).
- Discuss options for leveraging **advice and other services** offered through other government agencies including DHS with the responding FBI team.

### Recovery & Follow up

- **Share feedback on your experiences** with the local DOJ and FBI representatives. Consider conducting an after action review to discuss learnings to improve plans and performance in anticipation of future events.

\* Notify the FBI through the local Cyber Task Force or CyWatch (24/7) at 855-292-3937 or [CyWatch@fbi.gov](mailto:CyWatch@fbi.gov)

**Notify the FBI through the local Cyber Task Force or  
CyWatch (24/7) at 855-292-3937 or [CyWatch@fbi.gov](mailto:CyWatch@fbi.gov)**

offices can provide surge support and expertise as necessary, as each field office maintains personnel specifically trained on responding to incidents involving critical infrastructure and control systems. The response team may be further augmented by specialty support from FBI headquarters. For example, the FBI Cyber Action Team ("CAT") is the agency's elite rapid response force. On-call CAT members are prepared to deploy globally to bring their in-depth cyber intrusion expertise and specialized investigative skills to bear in response to significant cyber inci-

idents. CAT's management and core team are based in the Washington, D.C. metro area and are supplemented by carefully selected and highly trained field personnel. The FBI also has technical analysis and operations units that directly support the response team through deep-dive malware analysis and digital forensics, and by implementing custom-built technical solutions to advance an investigation.

If a cyber incident generates physical impacts rising to the level of a crisis, the FBI has ex-

tensive crisis management capability. The FBI Crisis Management Unit coordinates the FBI's tactical and disaster relief efforts. The unit also provides the capability to activate command posts anywhere in the United States, and coordinates the FBI's vast investigative resources and infrastructure to support large-scale incidents regardless of type.

Finally, the FBI maintains a fleet of aircraft to support deployments when an immediate response is necessary, as well as command post vehicles to support on-scene operations.

## Conclusion

The Department stands ready to assist victims of cyberattacks. By leveraging our field-centric model, investigative expertise, and partnerships at home and abroad, the Department works to pursue malicious cyber actors and to predict and prevent future attacks. We must continue to build trusting relationships and to work collaboratively to address the global cyber threat, and to impose costs on nation states, cybercriminals, and other malign cyber actors.

## NOTES

<sup>1</sup> See “Sector Specific Agencies,” U.S. DEPT. OF HOMELAND SECURITY (July 11, 2017), available at: <https://www.dhs.gov/sector-specific-agencies> (last accessed June 29, 2018) (describing the “16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof,” and listing the “Sector-Specific Agency” associated with each of these critical infrastructure sectors).

<sup>2</sup> “The Cost of Malicious Cyber Activity to the U.S. Economy,” COUNCIL OF ECON. ADVISORS, EXEC. OFFICE OF THE PRESIDENT, at 33 (Feb. 2018), available at: <https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf> (last accessed June 29, 2018).

<sup>3</sup> See “Presidential Policy Directive—United States Cyber Incident Coordination,” THE WHITE HOUSE (July 26, 2016) (“PPD-41”), available at: <https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident> (last accessed

June 29, 2018) (defining a “cyber incident” as “[a]n event occurring on or conducted through a computer network that actually or imminently jeopardizes the integrity, confidentiality, or availability of computers, information or communications systems or networks, physical or virtual infrastructure controlled by computers or information systems, or information resident thereon. For purposes of [PPD-41], a cyber incident may include a vulnerability in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.”).

<sup>4</sup> See “NCCIC Cyber Incident Scoring System,” U.S. COMPUTER EMERGENCY READINESS TEAM, available at: <https://www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System> (last accessed June 29, 2018).

<sup>5</sup> A “significant” cyber incident is one “that is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.” See PPD-41, *supra* note 3.





---

## CHAPTER 5

### TRAINING AND MANAGING OUR WORKFORCE

To appropriately identify, disrupt, dismantle, and deter computer intrusions and cyber-enabled crimes, the Department must develop and maintain a broad cadre of highly trained prosecutors, agents, and analysts. Whether identifying and locating cyber threat actors; collecting vital evidence through lawful process; or developing the latest tools to overcome sophisticated technologies criminals use to conceal their activities, Department personnel must understand how technology both facilitates criminal activity and can be used to detect, disrupt, and dismantle the same activity.

Investigators, for example, require advanced tools and resources to stay at least one step ahead of increasingly sophisticated anonymizing technologies that criminals and other adversaries exploit to avoid detection. Meanwhile, forensic analysts must possess the latest know-how to extract key evidence from sophisticated electronic media, such as encrypted cell phones and hard drives. Finally, prosecutors must tackle complex questions regarding legal authorities, jurisdiction, privacy, and other issues raised by investigating cybercrime and prosecuting those responsible for it.

The Department pursues two objectives in developing its workforce and specialized training initiatives. First, we seek to cultivate a multitude of attorneys who, in addition to superior legal skills, have the technologi-

cal background and experience necessary to make appropriate decisions in technology cases. Second, we seek to retain a group of non-lawyer professionals whose primary expertise is technology. These computer scientists, engineers, and digital forensic investigators collaborate with attorneys and investigators, together forming a team with all necessary skills. Cultivating a workforce of technologically-savvy employees requires care in hiring and training, but also, crucially, requires that the Department make the right decisions about how it manages and organizes its employees.

How the Department internally organizes itself, and especially how it assigns cyber work, is a central part of the strategy to carry out its critical cyber mission and to recruit, train, and retain a technologically-expert workforce. In some respects, this challenge is not new. For example, prosecuting environmental crimes requires mastery both of a complex area of law and of relevant scientific facts; likewise, prosecuting antitrust and other complex business cases requires in-depth knowledge of how industries operate. The Department's solution to these challenges has been to build headquarters components and networks of attorneys and investigators that specialize in these technical areas of law enforcement. A similar strategy has worked well for cyber cases: the Department has concentrated its work of identifying, dismantling, disrupting, and

deterring computer intrusions and other cyber-enabled crimes into a select number of headquarters components and into networks of specialized attorneys and investigators. This method of organization yields at least three benefits for recruitment, training, and retention—which, in turn, benefits the investigation and prosecution of cyber cases.

First, despite ever-increasing competition in the technology job market, the Department can attract skilled prospects who are inspired by our mission. The Department now has employees who, in addition to being excellent lawyers or investigators, also have deep experience in network defense, computer forensics, and software engineering. These employees very often came to work at the Department precisely because they wanted to work on cyber cases. Offering prospective employees the chance to work exclusively (or near-exclusively) in the rewarding and challenging field of computer crime is a significant recruiting advantage. But making that promise is credible only if the Department can offer employment in specialized units, where cyber work has been concentrated.

Second, training employees in cyber cases requires far more than classroom instruction or reading from textbooks. Every seasoned attorney and investigator knows that the bulk of his or her expertise came from practical, on-the-job experience. Because the Department's specialized cyber units both at headquarters and in the field expose attorneys and investigators to cyber investigations, and do so repeatedly, they build skills and human capital much more effectively

than if the work were dispersed indiscriminately around the Department.

Finally, the Department is constantly working to retain experienced attorneys and investigators in government employment. The skills of cyber investigators and attorneys are in heavy demand in the private sector, where salaries are much higher. The Department will lose this competition for talent if the only consideration is salary. Fortunately, that is not the only consideration for most employees. Only public service provides employees with so great an opportunity to protect and defend their country; in many ways, the work is itself a reward. To make maximum use of that reward, however, the Department's talented cyber workforce needs to be given regular opportunities to work on the cases and subject matter they feel most passionate about. Only an arrangement of specialized offices can offer that benefit.

In this spirit, the Department's criminal law enforcement entities, its United States Attorneys' Offices, and its relevant litigation divisions have dedicated workforce units and training initiatives that anchor the Department's broader strategy to recruit, train, and retain a technologically expert workforce in order to carry out its core cyber mission. These units and their specialized training initiatives are described below.

### ***1. Federal Bureau of Investigation***

As described in Chapter 4, the FBI is often a “first responder” to a cyber incident. With Cyber Task Forces located in each of its 56

field offices across the country, the FBI is prepared to respond to and investigate cyberattacks and intrusions wherever they may occur. Its agents serve both as investigators and high-tech specialists, capable of applying the most current technological know-how to collect evidence at the scene of a cyberattack or intrusion, analyze data forensically, and trace a cybercrime to its origins. Through its Cyber Division located at FBI headquarters in Washington, D.C., and the Operational Technology Division located at Quantico, Virginia, the FBI provides leadership to its global efforts to investigate cyber threats, whether they stem from criminal or national security actors. The Cyber Division has organized itself, both at headquarters and in FBI field offices, to focus its investigations and operations exclusively on computer intrusions and attacks, and related online threats.

The FBI is also responsible for the operation of the National Cyber Investigative Joint Task Force (“NCIJTF”), a multi-agency cyber center that serves as the national focal point for coordinating cyber investigations across government agencies. The NCIJTF is comprised of 30 plus partnering agencies from across law enforcement, the intelligence community, and the Department of Defense, with representatives who are co-located and work jointly to accomplish the organization’s mission from a whole-of-government perspective. Members have access to and analyze data that provides a unique, comprehensive view of the Nation’s cyber threat while working together in a collaborative environment in which they maintain the authorities and responsibilities of their

home agencies. The NCIJTF coordinates, integrates, and shares cyber threat information to support investigations and operations for the intelligence community, law enforcement, military, policy makers, and trusted foreign partners in the fight against cyber threats. The NCIJTF is responsible for coordinating whole-of-government cyber campaigns, integrating domestic cyber data, and sharing domestic cyber threat information.

The FBI Criminal Investigative Division has created the Hi-Tech Organized Crime Unit (“HTOCU”) to launch a long term, proactive strategy to target transnational organized crime groups using advanced technology to conduct large scale computer-enabled and computer-facilitated crime. HTOCU works to bring traditional organized crime techniques, tradecraft, and strategies to bear on transnational criminal enterprises that use high technology to perpetrate criminal activity. HTOCU, in coordination with the FBI’s Cyber Division and the Money Laundering Unit, has developed and implemented strategies to dismantle transnational criminal enterprises engaged in large-scale fraudulent activity. Furthermore, HTOCU works to identify new sources, technical vulnerabilities, collection opportunities, and emerging trends in cyber-enabled transnational organized criminal activity.

The Joint Criminal Opioid Darknet Enforcement (“J-CODE”) Team is a new FBI initiative, announced by Attorney General Sessions in January 2018, to target drug trafficking—especially fentanyl and other opioids—on the Dark Web. Building on the work that



began with the government's dismantling of Silk Road and AlphaBay, the FBI is bringing together agents, analysts, and professional staff with expertise in drugs, gangs, health care fraud and more, as well as federal, State, and local law enforcement partners from across the U.S. government, to focus on disrupting the sale of illegal drugs via the Dark Web and dismantling criminal enterprises that facilitate this trafficking. The J-CODE will create a formalized process to prioritize dark markets, vendors, and administrators for strategic targeting; to develop strategies to undermine confidence in the Dark Web; and to formulate de-confliction and operational requirements with other domestic and international partners.

In accordance with the requirements set forth in the Federal Cybersecurity Workforce Assessment Act of 2015, the Department, including the FBI, is identifying and coding federal positions that perform information technology, cybersecurity, and other cyber-related functions based on the work roles described in the National Initiative for Cybersecurity Education Framework.<sup>1</sup> This analysis will underpin an effort to prioritize areas of critical need within the workforce, and support possible recommendations for introducing new job roles that will improve the FBI's ability to respond to Internet-enabled crimes and technologically advanced threat actors.

With respect to training, the FBI has a number of programs to ensure its workforce possesses the key cyber skills and tools to succeed in their investigations, especially as

the technological landscape rapidly evolves. For instance, the FBI is implementing the "Cyber Certified" training and certification program for investigators, intelligence analysts, technical specialists, and attorneys, whether currently in the Cyber Program or working in other mission areas. These employees will be observed for future training and development activities.

In an attempt to rapidly increase the level of cyber knowledge shared throughout the organization, and in an effort to infuse cyber knowledge into traditionally non-cyber programs, the FBI has also created the Workforce Training Initiative ("WTI"). The WTI is designed to increase the number of employees who are capable of responding to, investigating, and analyzing a variety of cyber-related cross-programmatic matters, and its courses cover the breadth of cyber-related topics.

The On the Job Training ("OJT") initiative is a combination of classes and real world experiences encountered daily on a cyber squad. The OJT program takes place over a six-month period and requires a full-time commitment from participants. The participants are reassigned to a cyber squad and are expected to work cyber cases under the mentorship of cyber-skilled professionals. At the conclusion of the six-month program, participants return to their original squads with enhanced cyber skills to address cyber threats within that program and to share their knowledge. Upon completion of this program, participants will be designated Cyber Certified.

The FBI Digital Forensics program offers digital evidence related training and certifications to personnel dedicated to managing digital evidence challenges, and also offers technical training to the broader FBI workforce which familiarizes them with the challenges of properly preserving and handling digital evidence. The Forensic Examiner certification program includes over ten weeks of total training, practical exercises, mentorship, and a moot court which includes Department attorneys and senior examiners.

The FBI's Cyber Executive Certification Program provides high-level cyber training and prepares executives for their role in the cyber investigation process. Participants have the opportunity to obtain two industry standard certifications, in addition to the internal FBI certificate. Additionally, the digital evidence program offers advanced training to personnel supervisors of digital evidence workforce, preparing them to ensure the technical requirements of FBI investigation are met by the digital evidence staff.

Finally, FBI-led cyber training takes place at Cyber Academy campuses located at different points in the country, while digital evidence training occurs at Regional Computer Forensics Laboratories, and at FBI headquarters. Cyber training ranges from the Cyber Basic School, a two-week curriculum designed to instill cybersecurity fundamentals in all employees, to advanced training for seasoned cyber investigators. Digital evidence training includes guidance in analy-

sis of Windows, Macintosh, UNIX, and mobile operating systems, Internet artifacts, secure device access, vehicle forensics, and Internet of Things related challenges.

## **2. The Criminal Division**

### ***Computer Crime and Intellectual Property Section***

In 1996, the Department consolidated the Criminal Division's expertise in computer crime matters into a single office called the Computer Crime and Intellectual Property Section ("CCIPS"), with prosecutors devoted to pursuing computer crime prosecutions fulltime. Over the years, CCIPS's mission has grown beyond prosecution to include spearheading cyber policy and legislative initiatives, training and support, public outreach, and cybersecurity guidance. CCIPS consists of a team of specially trained attorneys dedicated to investigating and prosecuting high-tech crimes and violations of intellectual property laws, and to advising on legal issues concerning the lawful collection of electronic evidence.

Today, CCIPS is responsible for implementing the Department's national strategies to combat computer and intellectual property crimes worldwide by working with other Department components and government agencies, the private sector, academic institutions, and foreign counterparts, among others. Section attorneys work to improve the domestic and international legal, technological, and operational legal infrastructure to pursue network criminals most effective-

ly. Working in support of and alongside the 94 U.S. Attorneys' Offices ("USAOs"), CCIPS prosecutes violations of federal law involving computer intrusions and attacks. CCIPS has also worked with the Treasury Department's Office of Foreign Asset Control to use new authorities under Executive Order 13694 to bring sanctions against foreign nationals for malicious cyber-enabled criminal activities. In conjunction with the Executive Office for United States Attorneys ("EOUSA"), described below, CCIPS conducts at least four multi-day in-person trainings and up to twelve webinars a year. It also maintains an internal website with information available to all Department components that is visited more than 90,000 times a year, and has a rotating daily duty-attorney system that responds to approximately 2,000 calls for advice a year.

In addition, the Criminal Division established the Computer Hacking and Intellectual Property ("CHIP") coordinator program in 1995 to ensure that each USAO and litigating division has at least one prosecutor who is specially trained on cyber threats, electronic evidence collection, and technological trends that criminals exploit. The CHIP network now includes approximately 270 prosecutors from USAOs and Main Justice, and aids in the coordination of multi-district prosecutions involving cyber threats. Specialized CHIP units exist in 25 designated USAOs. CHIP Assistant U.S. Attorneys (AUSAs) work with law enforcement partners from multiple law enforcement agencies at the outset of an investigation, often in consultation with CCIPS, to provide legal guidance, help craft an investigative plan, obtain

necessary search warrants and court orders, collect electronic evidence, and ultimately, build a criminal case. Pursuant to departmental regulation, U.S. Attorneys are responsible for ensuring that experienced and technically-qualified AUSAs serve as the district's CHIP prosecutors; ensuring that CHIP resources are dedicated to CHIP program objectives; ensuring that the USAO notifies, consults, and coordinates with CCIPS and other USAOs; and promoting and ensuring effective interaction with law enforcement, industry representatives, and the public in matters relating to computer and intellectual property crime.

#### *Money Laundering and Asset Recovery Section*

The Criminal Division's Money Laundering and Asset Recovery Section ("MLARS") leads the Department's asset forfeiture and anti-money laundering enforcement efforts. MLARS is responsible for, among other things, coordinating complex, sensitive, multi-district, and international money laundering and asset forfeiture investigations and cases; providing legal and policy assistance and training to federal, State, and local prosecutors and law enforcement personnel; and assisting Departmental and interagency policymakers by developing and reviewing legislative, regulatory, and policy initiatives.

With respect to cyber-enabled threats in particular, MLARS has established a Digital Currency Initiative that focuses on providing support and guidance to investigators, prosecutors, and other government agencies on cryptocurrency prosecutions and forfei-



tures. The Digital Currency Initiative will expand and implement cryptocurrency-related training to encourage and enable more investigators, prosecutors, and Department components to pursue such cases, while developing and disseminating policy guidance on various aspects of cryptocurrency, including seizure and forfeiture. Through the Initiative, MLARS will also advise AUSAs and federal agents on complex questions of law related to cryptocurrency to inform charging decisions and other prosecutorial strategies.

*Office of Enforcement Operations,  
Electronic Surveillance Unit*

Electronic surveillance is one of the most effective law enforcement tools for investigating many types of criminal enterprises, including cyber-based criminal enterprises that use electronic media and Internet-based technologies to perpetrate their crimes. The Electronic Surveillance Unit (“ESU”) in the Criminal Division’s Office of Enforcement Operations is responsible for reviewing all federal requests to conduct interceptions of wire, electronic, or oral communications pursuant to the Wiretap Act. ESU’s specialized attorneys provide suggested revisions and offer guidance to ensure that electronic surveillance applications meet all constitutional, statutory, and Department policy requirements. Every federal wiretap application must be approved by a senior Department of Justice official before it is submitted to a court, and ESU makes recommendations to those officials based on its review. Additionally, ESU attorneys regularly conduct webinars and in-person trainings, and provide legal advice to federal prosecutors

and law enforcement agencies on the use of electronic surveillance. They also assist in developing Department policy on emerging technology and telecommunications issues.

*Office of International Affairs*

The Criminal Division’s Office of International Affairs (“OIA”) returns fugitives to face justice, and obtains essential evidence for criminal investigations and prosecutions worldwide by working with domestic partners and foreign counterparts to facilitate the cooperation necessary to enforce the law, advance public safety, and achieve justice. Drawing upon a vast network of international agreements and its expertise in extradition and mutual legal assistance, OIA in recent years has worked with domestic and foreign law enforcement to hold cybercriminals accountable in U.S. courts and obtain the evidence needed to untangle complex transnational cybercrime schemes.

In addition to its work supporting investigations and prosecutions of cybercriminals, OIA uses mutual legal assistance to obtain electronic evidence for foreign and domestic law enforcement personnel. As the need to obtain electronic evidence in virtually every type of criminal case has burgeoned, OIA has worked to modernize its practice in this area by creating a team of attorneys and support personnel specially trained in obtaining electronic evidence, and by implementing process efficiencies to ensure swift attention to requests from prosecutors and police. OIA is also actively engaged in the policy, legislative, and multilateral arenas in which topics concerning access to electronic evi-



dence and law enforcement cooperation are discussed and debated to ensure that the Department's mission is advanced and that our law enforcement personnel get the tools they need to keep pace with ever-evolving threats. Consistent with these goals, OIA conducts regular training for U.S. prosecutors on the tools available to them to obtain evidence located overseas and to secure the return of fugitives. OIA also provides frequent regional and bilateral trainings to our foreign partners to bolster their ability to stop criminal activity before it reaches our shores.

### ***3. The National Security Division***

The investigation, disruption, and deterrence of national security cyber threats are among the highest priorities of the Department's National Security Division ("NSD"). These priorities come from a recognition that network defense alone is not enough to counter the threat. To the contrary, we must also impose costs on our adversaries using all of the U.S. government's lawfully available tools. This "all-tools" approach informs NSD's efforts to combat cyber threats to our national security, with the goal of deterring and disrupting cyber-based intrusions and attacks. In this context, national security cyber cases are those perpetrated by nation states, terrorists, or their agents or proxies, or cases involving the targeting of information that is controlled for national security purposes.

All NSD attorneys must take a cyber course within two years of joining the division. NSD also conducts annually a one-day cyber training in-house for all NSD employ-

ees, which is taught by NSD and CCIPS attorneys.

In addition, in 2012, NSD launched the National Security Cyber Specialist ("NSCS") network to equip USAOs around the Nation with prosecutors trained on national security cyber threats, such as nation-state cyber espionage activities and terrorists' use of technology to plot attacks. NSCS-Main is comprised of lawyers and other experts drawn from NSD's component sections and offices, as well as from CCIPS and ESU in the Criminal Division. NSCS-Main also coordinates as needed with other Department headquarters components, including the Civil Division, the Antitrust Division, the Office of Legal Policy, and the Office of Legal Counsel, and works closely with the Department's investigative components, including the FBI.

The NSCS Network also includes AUSAs in each of the USAOs; these AUSAs serve as their offices' primary points of entry for cases involving cyber threats to the national security and coordinate closely with NSCS-Main. NSD and CCIPS, in conjunction with EOUSA, provides annual training for NSCS members. The NSCS training covers a number of national security cyber topics to enhance the education of the prosecutors who handle these matters. In addition, through the National Security/Anti-Terrorism Advisory Council, there are approximately seven training courses conducted annually for national security prosecutors. Those trainings generally include a number of cyber-related sessions for national security prosecutors.

Finally, this year, for the first time, NSD is offering a Cyber Fellowship for those selected attorneys who applied to further their education on technology-related issues. Five attorneys were selected to participate in 2018 and have been attending a series of trainings offered by the FBI, the CIA, Carnegie Mellon University, and the SANS Institute. Those selected have also agreed to assist with training and other cyber initiatives at NSD.

#### *4. United States Attorney's Offices / Executive Office for United States Attorneys*

The United States Attorneys serve as the nation's principal litigators, under the direction of the Attorney General. There are 93 United States Attorneys stationed throughout the United States, Puerto Rico, the Virgin Islands, Guam, and the Northern Mariana Islands.<sup>2</sup> Each United States Attorney is the chief federal law enforcement officer of the United States within his or her particular jurisdiction. United States Attorneys conduct most of the trial work in which the United States is a party. Although the distribution of caseloads varies between districts, each USAO deals with every category of cases, including cybercrime prosecutions. As referenced above, the role of the CHIP AUSA was established to ensure that each USAO has personnel trained on cyber threats, electronic evidence collection, and technological trends exploited by criminals. Similarly, the NSCS program discussed above was designed to equip USAOs around the nation with prosecutors specially trained on national security cyber threats, such as nation state cyber espionage activities and terrorists' use

of technology to plan attacks. The USAOs also coordinate as needed with Department headquarters components, such as the Criminal and National Security Divisions, in a further effort to ensure the effectiveness of such cyber-oriented investigations and prosecutions.

EOUSA provides executive and administrative support for the 93 United States Attorneys. Such support includes legal education, administrative oversight, technical support, and the creation of uniform policies, among other responsibilities.

The National Advocacy Center, which EOUSA operates, provides numerous courses every year addressing a wide variety of cyber-related topics. These courses are attended by prosecutors from across the country and are tailored to address the training needs of attorneys with varying levels of experience handling cyber matters. Working with CCIPS and the National Security Division's Counterterrorism and Counterespionage sections, these cybercrime courses range from introductory to advanced level and have included training addressing the nature of computer forensics, the investigation of computer intrusions, and the use of electronic evidence, among other related topics. In short, each year, the Department trains hundreds of federal prosecutors in cybercrime and national security cyber matters.

In addition to these in-person training programs, EOUSA, through the Office of Legal and Victim Programs and the Office of Legal Education ("OLE"), sponsors additional cyber training, including webinars that are

broadcast nationwide. These webinars allow the Department to provide supplemental cutting-edge training and allow prosecutors to view these presentations from their own offices, while still enabling them to remotely ask the presenters questions and download related materials. For example, EOUSA sponsored a webinar discussing new provisions of a Federal Rule of Evidence relating to electronic evidence, immediately after those provisions became effective. Almost 1,000 Department employees viewed that program. Working closely with CCIPS and OEO, additional notable webinars have included programs addressing legal standards for obtaining cell phone location information, searching and seizing computers and other digital devices, cryptocurrency, and social media and online investigations, to name just a few.

OLE, working with CCIPS, has also issued standalone written materials that prosecutors can use for training and law enforcement purposes.

### ***5. Drug Enforcement Administration***

The DEA enforces the Nation's controlled substance laws and regulations. Through its participation in J-CODE and beyond, DEA is developing its expertise in Dark Market investigations. DEA's Operational Support Unit ("STSO") serves as the point of contact between DEA offices and the technology and communications industry, in order to identify, address, and resolve subpoena and related compliance issues, as well as other legal and regulatory issues. STSO also dis-

seminates to the field guidance relating to these issues. STSO is attempting to bring DEA employees into a more advanced awareness of today's cyber world, so they can adapt to that environment while performing the daily tasks of Internet research and investigations.

### ***6. INTERPOL***

The mission of INTERPOL Washington (United States National Central Bureau), is to advance the law enforcement interests of the United States as the official representative to the International Criminal Police Organization (INTERPOL); to share criminal justice, humanitarian, and public safety information between our Nation's law enforcement community and its foreign counterparts; and to facilitate transnational investigative efforts that enhance the safety and security of our Nation.

INTERPOL Washington leverages a network of 192 countries connected by a secure communications platform to share information for the purpose of enhancing international cooperation in all areas of criminal investigation, including cybercrime investigations. INTERPOL Washington maintains an office dedicated to advancing the cybercrime investigations of U.S. law enforcement by establishing and maintaining relationships with the heads of cybercrime units of other countries; sharing information through the secure communications platform to assist cybercrime investigations conducted by the agencies of the Department of Justice and the Department of Homeland Security; and

providing support to other federal, State, local, and tribal law enforcement agencies.

thereby also increasing our own capacity to thwart cyber threats.

### ***7. Foreign Government Training Initiatives***

In addition to training its own personnel, the Department also provides training and technical assistance to foreign governments to ensure that they are equipped to address their own domestic cyber threats. As countries develop their own capacity to address cyber issues, they are also better equipped to assist the United States in investigations involving criminal conduct emanating from within their own borders. The Department has maintained a robust program for encouraging foreign governments to develop their criminal and procedural laws to address emerging cybercrime threats and capabilities, consistent with the Budapest Convention on Cybercrime. As discussed in Chapter 3, the Budapest Convention—which the United States ratified over ten years ago—provides a legal framework for criminalizing key types of cybercrime, developing the tools necessary to investigate such crime, and establishing the network for rapid international cooperation that must exist to investigate and prosecute cyber actors wherever they are located.

Using a balanced approach of frank policy discussions with countries that have technical capabilities similar to our own, combined with multilateral training initiatives aimed at countries whose legal infrastructure for addressing cyber threats is in earlier stages of development, the Department has continued to improve the capacity of other countries to address cyber threats around the world,

### ***8. Department-Wide Cybersecurity Awareness Training***

In addition to the specialized units and training described above, the Department recognizes that cybersecurity effectiveness depends on everyone in the organization. Users are still one of the most attacked entities in the organization. Social engineering attacks (described in more detail in Chapter 2) come in many forms, are still effective, and can target anyone in the Department. As such, all Department employees must have a basic understanding of their responsibilities when handling the Department's information and accessing its information system, while being held accountable for abusing those responsibilities.

All Department personnel receive annual cybersecurity awareness training. In addition, all employees and contractors must sign the "Department of Justice Cybersecurity and Privacy Rules of Behavior (ROB) for General Users" agreement, which confirms that the employee or contractor completed the training and understands the applicable cybersecurity requirements and responsibilities. As the agreement makes clear, "each [Department] user is responsible for the security and privacy of [Department] information systems and their data."

Adequate training ensures that everyone within the Department has a basic understanding of the relevant threats, their role in protecting our information and information



systems, and how to detect and respond to cybersecurity events. Typical web-based training is most common; however, many training delivery mechanisms are used to get the broadest penetration of the material. For example, phishing exercises are conducted throughout the year, and in-person briefings and topic-specific training sessions are offered for special audiences and material.

Finally, the Department has also hosted a number of Department-wide trainings and awareness campaigns to educate the Department's workforce on privacy and cybersecurity. The Office of Privacy and Civil Liberties organizes an annual Privacy Forum, which gathers the Department's privacy officials to discuss current privacy and civil liberties

issues. In addition, the Department's Office of the Chief Information Officer hosts an annual Cybersecurity Symposium, which provides a forum for employees to gain an understanding of the latest trends in cybersecurity from federal and industry leaders. These events help educate the Department's workforce on the most current trends in information security and privacy.

While the Department employs a robust training program, we can do more to carry the Department into the future. Training can reinforce best practices, enable advanced threat detection, and improve security and safety across the Department as we all work to carry out its critical cyber mission.

## NOTES

<sup>1</sup> See National Institute for Standards and Technology, Special Publication 800-181, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework* (Aug. 2017), available at: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf> (last accessed June 29, 2018).

<sup>2</sup> One United States Attorney is assigned to each of the 94 judicial districts, with the exception of Guam and the Northern Mariana Islands, where a single United States Attorney serves in both districts.



---

## CHAPTER 6

### LOOKING AHEAD

**T**his report describes the most significant cyber threats our Nation faces, and catalogs the ways in which the Department confronts and combats those threats. As the discussion in previous chapters reveals, the Department has had many successes. At the same time, we face a number of challenges.

In this chapter, we further explore those challenges and identify specific areas for additional inquiry. We also outline eight key areas of future effort that will define the Department's work in the months ahead.

#### Specific Challenges

Each part of the Department's efforts to confront cyber threats—(1) preventing and responding to cyber incidents (Chapter 4); (2) investigating and prosecuting cyber-related crimes (Chapter 2); and (3) dismantling, disrupting, and deterring malicious cyber threats (Chapter 3)—bears its own unique challenges.<sup>1</sup>

Here, we describe those challenges and, where applicable, discuss how the Department has begun addressing the challenge or what actions we may yet take to sharpen our efforts. Where appropriate, we also highlight issues that require further consideration and development due to the complex or evolving nature of the threat.

#### *1. Challenges in Preventing and Responding to Cyber Incidents*

##### *Working with the Private Sector*

Virtually every instance of cyber-related crime implicates the private sector in some way, whether the private sector is the target of malicious cyber activity, the provider of technology or services through which cyber-crimes are committed or concealed, or the repository of evidence (such as communications) relating to cyber-enabled criminal activity. As such, the relationship that the Department, including the FBI, builds and maintains with the private sector is critical to our efforts to combat cybercrime. Fortunately, the Department and the private sector already have engaged in numerous formal and informal collaborations. Even so, the Department must deepen these relationships, particularly as technology evolves and the cast of service providers and technology manufacturers continues to change.

##### *a. The Computer Security Research Community*

The computer security research community—which is comprised of not only computer security companies but also individuals and organizations with expertise in computer security—has made valuable contributions to combating cyber threats by discovering



significant exploitable vulnerabilities affecting, among other things, the confidentiality of data, the safety of Internet-connected devices, and the security of automobiles. Some security researchers have also been allies in law enforcement efforts to dismantle cyber threats. For example, assistance with malware analysis and mitigation techniques has helped law enforcement conduct operations against various cybercriminals, including through botnet takedowns.

Even so, some in the computer security research community harbor concerns that law enforcement may misconstrue as criminal activity their methods of searching for and analyzing vulnerabilities. Some researchers have even expressed anxiety that such concerns have chilled legitimate security research.

To ensure the Department maintains and fosters a positive, collaborative working relationship with computer security researchers, the Department should consider potential legal options to encourage and protect legitimate computer security research. For instance, a three-year exemption to the Digital Millennium Copyright Act (“DMCA”)²—the result of rulemaking by the U.S. Copyright Office³—has allowed researchers to conduct vulnerability research on consumer products, including Internet of Things (“IoT”) devices. IoT devices are prime targets of cybercriminals for use in illicit activities like distributed denial of service attacks. Finding and repairing vulnerabilities in consumer devices is important and will likely become

even more important as IoT devices proliferate, perform more household tasks, and collect more data capable of being monetized by criminals.

The Copyright Office has initiated its next rulemaking process to evaluate extending the DMCA exemptions. The Department has submitted input to the Copyright Office in support of extending and expanding the current security research exemption, with caveats intended to protect public safety and avoid confusion over legal research activities.<sup>4</sup> At the same time, the Department should continue evaluating existing laws and regulations to identify other opportunities to support and encourage legitimate computer security research. Finally, the Criminal Division’s Cybersecurity Unit should conduct additional outreach to the computer security community. In doing so, the Unit should seek out opportunities to: (1) explain how the Department’s policies and practices address concerns about unwarranted prosecutions for legitimate security research; and (2) better educate the computer security research community about the federal criminal laws implicated by computer security activities.

*b. Encouraging Private Sector Reporting of Cyber Incidents*

Another important component of the Department’s collaboration with the private sector is the public-private work on information sharing and threat assessment. As discussed in Chapter 4, the FBI disseminates numerous reports directly to members of

the private sector to inform them of cyber threats. This information sharing provides the private sector with actionable intelligence that enables them to take appropriate precautions.

Information sharing, however, is most effective when it flows two ways. When a private sector entity reports a breach or attempted intrusion, the Department gains valuable insights into threat activity that can help direct, in real time, law enforcement efforts to investigate and disrupt the malicious activity. Prompt reporting also provides information that officials can accumulate and share with other private sector entities to facilitate appropriate security measures. Indeed, efforts by the Department and FBI to help manage cyber incidents and, later, to bring perpetrators to justice through prosecution are best accomplished when the victim—who may be the first to discover an incident—reports the incident or intrusion in a timely manner.

Unfortunately, many cyber incidents in the United States are never reported to law enforcement. Victims—especially businesses—often decide not to report cyber incidents for a variety of reasons, including concerns about publicity and potential harm to the company's reputation or profits, and even concerns of retaliation by a nation state where they wish to do business. Some victims may simply not know how to report the incident to appropriate authorities. And still others, particularly larger companies, may try to act on their own to pursue, confront, or disrupt the perpetrator, though doing so may trig-

ger civil or even criminal liability, or may impact U.S. foreign relations. Regardless of the reason, lack of reporting is a significant impediment to the Department's efforts to thwart cybercriminals and to address threats to national security—particularly when new threats are emerging.

Encouraging reporting from private sector victims is thus critical to enhancing the Department's ability to prevent, deter, investigate, and prosecute (or otherwise disrupt) cybercrimes. To facilitate reporting, the Department should consider not only how to build deeper trust with the private sector, but also understand and address the private sector's needs and concerns related to reporting. This assessment should include understanding how best to incentivize reporting as well as how to eliminate obstacles or barriers. The Department should also continue its outreach to the private sector to identify additional areas for collaboration, especially with respect to reporting and information sharing. In the past, such outreach has resulted in industry-targeted guidance such as the Criminal Division Cybersecurity Unit's *Best Practices for Victim Reporting and Responding to Cyber Incidents*.<sup>5</sup>

The Department must also consider the role that DHS and other government agencies play in working with the private sector to ensure federal agencies' efforts are complementary and cooperative. In addition to DHS and other federal partners, the Department should continue to work with the agencies that regulate the private sector to evaluate

expectations and encourage clear thresholds for reporting.

The Department's additional efforts on private sector reporting should also include attention to statutory data breach notification requirements. Currently, all 50 States have enacted separate notification laws setting standards governing notification by private entities when a data breach occurs, but there is no federal reporting requirement or standard. As such, companies must navigate and comply with the varying requirements in 50 State jurisdictions.<sup>6</sup> In the wake of recent high-profile data breaches exposing Americans' personal information, Congress has a revived interest in national notification requirements. A national data breach standard could increase federal law enforcement's effectiveness to pursue hackers and prevent data breaches.

*c. Reviewing Guidance on Victim Notification*

In 2012, the Attorney General issued General Guidelines for Victim and Witness Assistance ("AG Victim Guidelines" or "guidelines") that, among other things, discussed two statutes—the Victims' Rights and Restitution Act, 42 U.S.C. § 10607, and the Crime Victims' Rights Act, 18 U.S.C. § 3771—which accord certain rights to individuals who meet the statutory definition of "victim." The AG Victim Guidelines also address when FBI notification to victims and witnesses is appropriate and warranted. Given the evolving nature of cyber-enabled crimes—including the fact that it is not always easy to identify a cybercrime "victim" or the extent or nature

of the harm—the Department should review the AG Victim Guidelines to ensure, among other things, that the guidelines, and any related victim notification policies and practices, appropriately account for the unique and often nuanced nature of cybercrime.

*Preventing Cyber-Related Vulnerabilities in Connection with Foreign Investment and Supply Chains*

As part of its efforts to prevent cybercrime, the Department is concerned with mitigating vulnerabilities that threaten national security. Such areas concern foreign investment in domestic assets and foreign supply chains.

For example, a March 22, 2018 Presidential Memorandum observed that "China directs and facilitates the systematic investment in, and acquisition of, U.S. companies and assets by Chinese companies to obtain cutting-edge technologies and intellectual property and to generate large-scale technology transfer in industries deemed important by Chinese government industrial plans."<sup>7</sup> Under ambitious industrial policies, China aims to use foreign investment as a means of dominating cutting-edge technologies like advanced microchips, artificial intelligence, and electric cars, among others.

Currently, the Department responds to threats posed by foreign investment in the United States and the export of sensitive technology by enforcing U.S. export controls and through the Committee on Foreign Investment in the United States ("CFIUS"), a statutorily-established body that has au-

thority to review transactions that could result in control of a U.S. business by a foreign person. As the March 22, 2018 Presidential Memorandum indicates, further coordination through CFIUS, enforcement of existing technology transfer controls, and other interagency efforts will be necessary to tackle risks from foreign investment in sensitive industries and technologies.

In addition to foreign investment, the Department is generally concerned with hardening supply chains. Technology supply chains are especially vulnerable, because the hardware components and software code that go into technology products often come from foreign sources, including developers in Russia and China.<sup>8</sup> To address these concerns, the Department coordinates with other government agencies and the private sector to effectively manage and mitigate cybersecurity risks in U.S. supply chains.

For example, the Department contributes to Team Telecom, an ad hoc interagency working group that considers the law enforcement, national security, and public safety implications of applications for licenses from the Federal Communications Commission involving a threshold percentage of foreign ownership or control. Moving forward, the Department should continue to engage with these and other interagency efforts to determine the best ways to strengthen defenses against national security risks.

## ***2. Challenges in Investigating and Prosecuting Computer Crime***

### *Accessing Data in the United States*

Data not only is key to understanding the nature of cybercrime and the identity of perpetrators, but also is a primary source of evidence for prosecution. Unfortunately, the relevant data is often hard to reach, hidden on computers in different States or even in countries half a world away, lurking on dark markets, or protected by anonymized host servers or encryption. Recognizing that accessing data is the starting point and often the cornerstone of computer crime investigations and prosecutions, the Department has made concerted efforts to improve its ability to collect data related to criminal activity. However, several challenges to accessing data remain and require further collaboration with federal, State, and private sector partners.

One such challenge is the reality that cybercrime often does not take place in one identifiable, physical location. Sophisticated cybercriminals can control botnets spread throughout several States or countries and can hide their illegal activities on proxy networks. The rules governing law enforcement efforts, however, have largely not kept pace with these criminal realities. For this reason, the Department proactively engaged with the Federal Rules Committee and on December 1, 2016, an amended version of Rule 41 of the Federal Rules of Criminal Procedure went into effect. (That new Rule is discussed in detail in Chapter 3.)



The circumstances that the amendments to Rule 41 address are important, but they do not cover all instances where data related to criminal activity are stored in varying or unknown locations within the United States. The Department should identify any additional common or recurring circumstances where current legal authorities fall short of providing law enforcement with the tools necessary to access relevant data within the United States and determine whether changes similar to the recent Rule 41 amendments would be effective.

#### *Accessing Data Abroad*

The Department faces similar challenges in accessing data located outside the United States. As with the Rule 41 amendments in the domestic context, the Department recently engaged with partners to enhance our investigative authority in such circumstances. In particular, as the result of a joint effort between the private sector and the Department to bring clarity to investigative demands for data stored overseas, the Clarifying Lawful Overseas Use of Data Act (“CLOUD Act”) became law on March 23, 2018. (The CLOUD Act is also discussed in Chapter 3.)

Passage of the CLOUD Act institutes a framework for technology companies to comply with investigative demands for data stored outside of the requesting country’s territory, and creates processes to resolve thorny conflict of laws problems. The Act clarifies that the U.S. government’s traditional authority in this area remains in force: communications service providers must disclose infor-

mation subject to a court order that is within their “possession, custody, or control,” even if the electronic servers containing that information are located overseas. The CLOUD Act also authorizes our government to enter into formal agreements with other nations that remove legal barriers that would otherwise create conflict of laws problems where a provider is subject to a foreign court order to produce data stored in that other country. The Act requires both governments to “certify” that the laws and practices of the other country provide adequate protections for human rights and personal privacy. The agreements must also implement transparency measures and periodic reviews to ensure ongoing compliance. The Department is currently considering how it should implement such agreements.

Challenges remain, however, when investigating computer crimes that extend overseas, particularly because the CLOUD Act addresses only those instances where the relevant overseas data is possessed or controlled by an entity subject to U.S. jurisdiction. Many types of evidence fall outside those criteria, and traditional mutual legal assistance treaty (“MLAT”) procedures may also fall short.

For those reasons, the Department continually aims to improve its international outreach efforts and to engage with international Internet governance bodies to encourage them not to apply rules that unreasonably restrict or interfere with valid investigations. For example, the Department is currently monitoring and assessing the impact of the European Union’s sweeping General Data

Protection Regulation (“GDPR”), which went into effect on May 25, 2018.

Broadly speaking, the GDPR regulates how private companies and governments process, store, and transfer data concerning E.U. residents, including how such data and information is handled and transferred into and out of the E.U. Violators could be subject to fines up to 4% of their gross revenue worldwide or 20 million Euros, whichever is greater, creating a serious financial incentive for covered entities not to violate the new regulation. Exceptions written into the GDPR should ensure that it does not affect the ability of U.S. law enforcement to obtain evidence through MLATs. Also, law enforcement-to-law enforcement sharing is covered by a separate directive and is thus outside of the scope of the GDPR. Still, significant questions and uncertainties exist about the GDPR, which could negatively affect law enforcement, including by impeding information sharing.

For example, some interpret the GDPR to require that the publicly-available WHOIS system remove information about the registrants of Internet domain names from public access, thereby necessitating the building and maintenance of secured law enforcement portals to access that information. As described in Chapter 3, prosecutors and law enforcement agencies around the world use the WHOIS system thousands of times a day to investigate crimes ranging from botnets to online fraud. The registrant data in WHOIS can create crucial leads to targets’ identities, locations, and other pieces of their criminal infrastructure. This data can also help identify additional victims. Due to the significant

risk associated with noncompliance with the GDPR, however, the private organization responsible for maintaining WHOIS has decided to remove much of the registrant data from the publicly-available segments of the system while the organization works with stakeholders, including the Department, to develop a GDPR-compliant system.

This is only one example of how the GDPR may be interpreted to impede the ability of law enforcement authorities to obtain data critical for their authorized criminal and civil law enforcement activities. Uncertainty about the GDPR also has placed in question not only voluntary disclosures of information about criminal activity—*e.g.*, by their employees, contractors, or customers—to U.S. law enforcement agencies, but also may cause companies with a significant E.U. presence to become reluctant to comply even with disclosures required by legal process, such as warrants and subpoenas, for fear that such a disclosure would be in violation of the GDPR. Absent official guidance, companies with significant E.U. business may become reluctant to participate in mandatory data transfers to U.S. law enforcement and regulatory authorities, which would impede effective tax collection, limit the ability of agencies to stop anti-competitive business practices, impair the work of public health and safety agencies, and undermine the integrity of global banking, securities, and commodities markets. This could also undercut the Department’s mitigation programs for businesses and individuals that wish to cooperate in areas such as fraud, bribery, money laundering, sanctions violations, and antitrust matters—programs that yield information

that often results in criminal referrals, and thus relate to the Department's core mission.

In short, given the uncertainty that the GDPR presents in certain key areas, the Department (as well as the U.S. government as a whole) must continue to collaborate with European authorities and stakeholders to carefully monitor the GDPR's impacts.

### *The "Going Dark" Problem*

One of the most significant challenges to the Department's ability to access investigative data is the "Going Dark" problem. "Going Dark" describes circumstances where the government is unable to obtain critical information in an intelligible and usable form (or at all), despite having a court order authorizing the government's access to that information. The problem impacts a range of issues, including data retention;<sup>9</sup> anonymization; provider compliance (or absence thereof); foreign-stored data; data localization laws; tool development and perishability; and other similar issues. The challenges posed by the Going Dark issue have achieved greatest prominence in the context of encryption.

These challenges have significantly grown in recent years as the sophistication of encryption has increased. In the past, only the most sophisticated criminals encrypted their communications and data storage; today the average consumer has access to better technology than sophisticated criminals had twenty years ago. Previously, providers used encryption of some sort but generally retained a way of accessing the unencrypted data if necessary or desired, including to comply with law enforcement search warrants or

wiretap orders. In the past several years, the Department has seen the proliferation of default encryption where the only person who can access the unencrypted information is the end user. The advent of such widespread and increasingly sophisticated encryption technologies that prevent lawful access poses a significant impediment to the investigation of most types of criminal activity, including violent crime, drug trafficking, child exploitation, cybercrime, money laundering (including through cryptocurrencies), and domestic and international terrorism.

Faced with the challenges posed by encrypted information, investigative agencies have sometimes looked to other sources of information and evidence, which can be costly to procure and maintain. While these efforts have occasionally been successful, evidence and information lost to encryption often cannot be replaced solely by pursuing other sources of evidence. For example, communications metadata, such as non-content information about who contacts whom in phone records, can be helpful in putting the pieces together, but it provides less information than the content of data and communications—a difference that can prove outcome-determinative in the context of a criminal investigation, where prosecutors must prove guilt beyond a reasonable doubt. Moreover, metadata is also often simply unavailable because there is no mandate for providers to be able to access it. Relatedly, in the context of a judicial order authorizing the real-time interception of communications, the court must find, by law, that alternate sources of data do not exist or are insufficient to meet the investigation's goals.

## Going Dark

Warrant-proof encryption poses a serious challenge to effective law enforcement.

“To those of us charged with the protection of public safety and national security, encryption technology and its application... will become a matter of life and death which will directly impact our safety and freedoms.”

– FBI Director Louis Freeh  
July 9, 1997



1997

“We have engaged the tech community aggressively to help solve this problem. You cannot take an absolutist view on this. So if your argument is strong encryption, no matter what, and we can and should, in fact, create black boxes, then that I think does not strike the kind of balance that we have lived with for 200, 300 years.”

– President Barack Obama  
March 11, 2016



2016

“While convinced of the problem, I’m open to all constructive solutions, solutions that take the public safety issue seriously. We need a thoughtful and sensible approach, one that may vary across business models and technologies, but . . . we need to work fast.”

– FBI Director Christopher Wray  
March 7, 2018



2018



– U.K. Home Secretary Amber Rudd  
August 1, 2017

“To be very clear — the [U.K.] government supports strong encryption and has no intention of banning end-to-end encryption. But **the inability to gain access to encrypted data in specific and targeted instances is right now severely limiting our agencies’ ability to stop terrorist attacks and bring criminals to justice.**”

“Few issues have vexed law enforcement agencies more than this one. They can’t get access to the data they need to stop crime and hold criminals to account. **95 per cent of [our intelligence organization’s] most dangerous counter-terrorism targets actively use encrypted messages to conceal their communications.** We need access to digital networks and devices, and to the data on them, when there are reasonable grounds to do so. These powers must extend beyond traditional interception if our agencies are to remain effective and pre-empt and hold to account criminal activity. There will also need to be obligations on industry – telecommunications and technology service providers – to cooperate with agencies to get access to that data . . . .”

– Australian Minister for Law Enforcement & Cybersecurity Angus Taylor  
June 6, 2018





Exploiting software vulnerabilities can be another way to access encrypted (or otherwise inaccessible) data on a phone or other



*“Responsible encryption is achievable. Responsible encryption can involve effective, secure encryption that allows access only with judicial authorization. Such encryption already exists. Examples include the central management of security keys and operating system updates...”*

*—Deputy Attorney General  
Rod Rosenstein,  
October 10, 2017*

---

---

device. The Department has, in some instances, lawfully exploited security flaws to access electronic data, including data stored on smartphones. This is a promising technique, and the Department should expand its use in criminal investigations. However, so-called “engineered access” is not a replacement for all the evidence, including evidence subject to a court order, that is lost. Moreover, expanding the government’s exploitation of vulnerabilities for law enforce-

ment purposes will likely require significantly higher expenditures—and in the end it may not be a scalable solution. All vulnerabilities have a limited lifespan and may have a limited scope of applicability. Software developers may discover and fix vulnerabilities in the normal course of business, or the government’s use of a vulnerability could alert developers to its existence. Finally, each vulnerability might have very limited applications—limited, for example, to a particular combination of phone model and operating system.

The challenges posed by the Going Dark problem are among law enforcement’s most vexing. To address these challenges, the Department’s efforts should include: (1) considering whether legislation to address encryption (and all related service provider access) challenges should be pursued; (2) coordinating with international law enforcement counterparts to better understand the international legal, operational, and technical challenges of encryption; (3) collecting accurate metrics and case examples that demonstrate the scope and impact of the problem; (4) working to use technical tools more robustly in criminal investigations; (5) insisting that providers comply with their legal obligations to produce all information in their possession called for by compulsory process, and holding them accountable when they do not; (6) working with State and local partners to understand the challenge from their perspective and to assist them technologically in significant cases; and (7) reaching out to academics, industry, and technologists to fully understand the implications and possibilities for lawful access solutions.

### *Additional Investigative Authorities*

The Department has identified at least two additional legal authorities it needs to support cyber-related investigations. First, exceptions to the court order requirements of the Pen Register statute, 18 U.S.C. § 3121, are unnecessarily narrow. That statute governs the real-time collection of non-content “dialing, routing, addressing, or signaling information” associated with wire or electronic communications. This information includes phone numbers dialed as well as the “to” and “from” fields of e-mail. In general, the statute requires a court order authorizing collection of such information on a prospective basis unless the collection falls within a statutory exception. The exceptions to the Pen Register statute, however, are not coextensive with the exceptions to the Wiretap Act, codified at 18 U.S.C. § 2511 *et seq*, which generally governs wiretaps to obtain the content of wire or electronic communications. This results in the illogical situation where non-content information associated with a communication is subject to more extensive protection than the content of the communication itself. Moreover, the Pen Register statute’s consent provision could be clarified to allow users to provide direct, express consent for implementation of a pen/trap device by the government to facilitate cooperative investigation efforts. The Department stands ready to assist Congress in developing legislation to implement this needed improvement.

Second, the Department faces similar problems in obtaining electronic communication transactional records (“ECTRs”)—the e-mail equivalent of toll billing records for

telephone calls<sup>10</sup>—in national security investigations. ECTRs do not include the content of communications, but they can provide crucial evidence early in national security investigations, when investigators do not yet have a clear indication of a subject’s network of contacts. Information obtained from ECTRs, such as e-mail addresses, can help establish the probable cause necessary to get a Foreign Intelligence Surveillance Act order or search warrant to allow the FBI to obtain the content of stored communications, identify a potential confidential human source who may be able to provide valuable intelligence, or help eliminate a subject from suspicion. As electronic networks increasingly have supplanted telephone networks as the means for terrorists and foreign agents to communicate, the ability to access these records efficiently has become even more important to the FBI’s work.

Under 18 U.S.C. § 2709, electronic communication service providers are obliged to provide ECTRs in response to certain requests—sometimes called National Security Letters (“NSLs”)—made in connection with qualifying national security investigations. Companies, however, have invoked an omission in section 2709 to refuse to provide ECTRs in response to NSLs. The statute states in paragraph (a) that wire or electronic communication service providers have a duty to provide ECTRs in response to a request made by the Director of the FBI under paragraph (b). But paragraph (b) fails expressly to include ECTRs in the categories of information the Director may request, even though paragraph (a) explicitly references ECTRs.

Clarifying the statutory authority would strengthen the Department's ability to conduct counterintelligence investigations and to identify and disrupt terrorist plots in the United States. Law enforcement has obtained equivalent telephone records with a simple subpoena for decades, and the courts have held that non-content metadata of this kind, held by third-party service providers, is not protected by the Fourth Amendment.<sup>11</sup> A proposal to clarify that the FBI may obtain ECTRs by issuing NSLs would reaffirm a similar type of authority to the equivalent type of electronic communications information.

#### *Apprehending Criminals Located Abroad*

Even when accessible data allows law enforcement to understand the nature of the crime, to identify potential perpetrators, and to build a case for prosecution, holding the guilty party or parties accountable can still be a challenge. While the Department has made several advances to enhance its ability to prosecute sophisticated cybercriminals, difficulties apprehending criminal suspects, as well as the need for additional prosecutorial authorities, continue to hinder our efforts to bring malicious cyber actors to justice.

For example, as with our successful effort to amend Rule 41, the Department worked with the Federal Rules Committee to tackle the problem of serving criminal defendants accused of committing computer crimes. Rule 4 governs the service of criminal process upon individuals and organizations—essentially the process by which prosecutors give notice of charges to, and initiate court

proceedings against, a criminal defendant. Prior to the amendment, Rule 4 did not explicitly provide a method to serve process on an organization with no physical presence in the United States, an artifact of the pre-cyber era when organizations could hardly commit crimes in the United States without having a physical presence here. As discussed in Chapters 2 and 3, today, technology allows foreign actors to commit intellectual property and computer crimes in the United States from virtually anywhere in the world.

Rule 4, amended as of December 1, 2016, now provides prosecutors with a “non-exhaustive list of methods” for serving “an organization not within a judicial district of the United States.” Most importantly, the amended Rule 4 allows the government to serve a foreign organization “by any . . . means that gives notice.” For example, the government has relied on the amended Rule 4 to serve foreign organizations by mailing and e-mailing process to the foreign organization's U.S.-based defense counsel. The government has also served foreign organizations by mailing process to the registered agent for a recently dissolved U.S. subsidiary of the foreign organization or, in another case, by personally serving process on the president of a U.S. organization that shared a common “parent” organization with the subject of the summons. This change is particularly important in situations where a state-owned enterprise is charged with a crime but the foreign jurisdiction is unwilling to assist with efforts to serve process.

Service, however, is only one facet of the problem that the Department faces in at-



tempting to hold sophisticated cybercriminals accountable. As noted throughout this report, attributing a cyber-incident to an individual or group of actors is difficult due to anonymizing technologies and encryption techniques that allow cybercriminals to remain hidden from law enforcement. Additionally, there are cybercriminals who, though identified, manage to remain beyond the reach of U.S. law enforcement, especially when they are located abroad. While the Department has several mechanisms to bring cybercriminals to the United States to face trial, including extradition treaties and collaborative relationships with other countries (see Chapter 3), these efforts are not always successful. Some foreign sovereigns choose not to cooperate or will do so only after imposing unreasonable limitations on law enforcement. Other countries may not punish perpetrators for the specific computer crime the United States is seeking to prosecute or may lack sophisticated domestic cybercrime law enforcement capabilities. In addition to continuing to build strong relationships with other countries and assisting their efforts to meet the requirements to join the Budapest Convention (also discussed in Chapter 3), the Department should continue to identify necessary additional authorities and potential mechanisms for bringing foreign-based cybercriminals to justice.

#### *Additional Criminal Prohibitions*

Once malicious cyber actors are identified, it is important for the Department to have the authorities necessary to prosecute those individuals for the illicit activity. Additional criminal prohibitions would help the De-

partment prosecute and deter malicious cyber activity.

#### *a. Protecting Election Computers from Attack*

The principal statute used to prosecute hackers—the Computer Fraud and Abuse Act (“CFAA”)—currently does not prohibit the act of hacking a voting machine in many common situations. In general, the CFAA only prohibits hacking computers that are connected to the Internet (or that meet other narrow criteria for protection). In many conceivable situations, electronic voting machines will not meet those criteria, as they are typically kept off the Internet. Consequently, should hacking of a voting machine occur, the government would not, in many conceivable circumstances, be able to use the CFAA to prosecute the hackers. (The conduct could, however, potentially violate other criminal statutes.)

#### *b. Insider Threat/Nosal Fix*

Until recently, the Department regularly used the CFAA’s prohibition on “exceeding authorized access” to prosecute insider threats—in particular, employees who abused permitted access to their employers’ systems by stealing proprietary information or accessing information for their own illicit purposes and gain. The Department, for example, prosecuted police officers who sold their access to confidential criminal records databases, government employees who accessed private tax and passport records without authority, and bank employees who abused access to steal customers’ identities. These employees had



some right to access those computers, but their conduct was a crime under the CFAA because they intentionally exceeded their employer's computer use rules.

Decisions in the Second, Fourth, and Ninth Circuit Courts of Appeals, however, have limited the definition of "exceeds authorized access" in section 1030(e)(6) of the CFAA. In *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc), the Ninth Circuit held that an indictment did not state a violation of the CFAA when it alleged that a former employee had asked current employees to access information in a proprietary database to aid him in starting a new firm. The company had computer policies that limited employee access to legitimate work purposes. Although the employees' efforts to access information for the benefit of the former employee's new firm violated the company's policies, the court held such an activity did not violate federal criminal law. According to the *Nosal* court, the definition of "exceeds authorized access" in section 1030(e)(6) "is limited to violations of restrictions on access to information, and not restrictions on its use." *Id.* at 863-64.<sup>12</sup>

Such decisions have caused grave damage to the government's ability to prosecute and protect against serious insider threats. If the CFAA can be used only against outsiders with no right at all to access computers, many insider threats—including those in the intelligence and law enforcement communities with access to extremely sensitive information—may go unpunished. Prosecutors should have adequate statutory authority to pursue insiders who abuse their computer

access for illicit means. Any such authority should also ensure appropriate consideration and treatment of legitimate privacy-related concerns.

#### *c. CFAA as RICO Predicate*

As discussed in Chapter 3, the Racketeer Influenced and Corrupt Organizations Act ("RICO") is an important prosecutorial tool for charging organizations engaged in a pattern of criminal activity because RICO violations carry substantial sentencing penalties as well as the ability for the government to seize assets of the criminal organization. RICO requires proof of, among other things, a pattern of "racketeering activity," which is defined as violations of two or more qualifying predicate criminal acts.

Currently, computer fraud under the CFAA does not qualify as a predicate act under the RICO statute, whereas similar conduct, such as wire fraud and mail fraud, does qualify. Adding the CFAA as a predicate offense for RICO purposes could increase our ability to fight cybercrime and take down criminal organizations engaged in such activities.

#### *d. Combating Sextortion*

"Sextortion" and related offenses are discussed in Chapter 2. Although such conduct may implicate certain existing criminal laws, there are no federal criminal statutes specifically addressing sextortion and non-consensual pornography. Additionally, while stalking, bullying, and harassment have more commonly been dealt with by local law enforcement or outside the criminal justice

system, the use of computers and mobile networks has turned many such crimes into multi-jurisdictional and even multi-national offenses.<sup>13</sup> The increasingly expansive nature of these crimes, in addition to the use of new technologies, may merit a federal response. New federal criminal offenses specifically targeting sextortion and non-consensual pornography, as well as possible new sentencing enhancements for such offenses under existing authorities, could have merit.

### ***3. Challenges in Connection with Other Legal Actions to Dismantling, Disrupting, and Deterring Malicious Cyber Conduct***

As described in Chapter 3, in addition to traditional investigation and prosecution, the Department has an array of other techniques and tools to dismantle, disrupt, and deter cyber threats, including a blend of civil, criminal, and administrative powers. The Department has employed these tools to disable botnets, disrupt dark markets, and pursue sanctions against specified malicious actors. As with our investigation and prosecution activities, however, the Department needs additional tools and authorities to maximize effectiveness.

#### ***Tackling Tor/Dark Markets***

The Department cannot disrupt cyber activity that it cannot find. This makes Tor and the existence of dark markets one of the greatest impediments to our efforts. As discussed in detail in Chapter 2, Tor provides anonymity in two ways—first, by anonymizing com-

munications sent from computers running Tor, and second, by allowing individuals to operate websites on the Dark Web called Tor “Hidden Services” without divulging location information of the websites’ servers.

While sometimes used for innocuous and even beneficial purposes, the anonymity afforded by Tor also poses a unique and significant threat to public safety. The anonymizing technology is effective, making it difficult to identify the physical location of dark market websites either to shut them down or to identify who is administering them. The result is that law enforcement investigators can observe and document the fact that disturbing criminal activity is occurring, but they cannot use the sort of investigative steps that ordinarily would allow them to determine who is perpetrating the crimes.

Combating criminals’ abuse of Tor and their exploitation of dark markets requires a concerted effort. The Department should work with partners to develop new technological tools that will enable law enforcement to identify the true location of Hidden Services websites engaged in criminal activity. Effective development and use of these tools will enable law enforcement to locate and lawfully seize servers hosting such sites, and to identify the administrators, vendors, buyers, and participants who use them. In addition, the federal government should carefully evaluate its role in funding these anonymizing technologies, as currently the U.S. government is the primary source of funding for the Tor Project, the organization responsible for maintaining the Tor software.

*Enhancing Our Ability to Disrupt Botnets*

On May 22, 2018, DHS and the Department of Commerce released a joint report titled, “A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats.”<sup>14</sup> The report encourages collaboration between the government and private industry, recognizing that addressing the global botnet problem requires further discussions on market incentives and on securing products at all stages of their life cycle. The Department should play an active role in these efforts.

Despite being the principal law enforcement agency tasked with disrupting and dismantling botnets, the Department’s current statutory authority is limited. As it stands today, the law gives federal courts the authority to issue injunctions to stop the ongoing commission of specified fraud crimes or illegal wiretapping through the use of botnets, by authorizing actions that prevent a continuing and substantial injury. The Department used this authority effectively in its successful disruption of the Coreflood botnet in 2011 and of the Gameover Zeus botnet in 2014. *See* Appendix 2. Because the criminals behind these particular botnets used them to intercept communications containing online financial account information and, with that information, committed fraud, the existing law allowed us to obtain court authority to disrupt the botnets by stopping the criminals’ commands from reaching the infected computers.

Unfortunately, botnets can be and often are used for many other types of illegal activity beyond fraud or illegal wiretapping. As explained in Chapter 2, for example, malicious actors can employ botnets to steal sensitive corporate information, to harvest e-mail account addresses, to hack other computers, or to execute DDoS attacks against websites or other computers. When these crimes do not involve fraud or illegal wiretapping, courts may lack the statutory authority to issue an injunction to disrupt the botnet. The Department should evaluate the merits of creating a more comprehensive authority for courts to address all types of illegal botnets.

*Advancing a CFAA Forfeiture Fix*

As discussed in Chapter 3, the Department in recent years has regularly used civil forfeiture authorities to disrupt cybercriminal groups by seizing valuable assets such as computer servers and domain names used to operate botnets, as well as profits derived from illegal activity.<sup>15</sup> These actions are permissible even when it is not yet possible to arrest the offenders. Expanding forfeiture authority to CFAA offences could enhance the Department’s capacity to dismantle, disrupt, and deter cyber threats by targeting the instruments of, and profits from, cybercrime.

**Issues for Further Evaluation**

In addition to helping facilitate action on the specific recommendations made above and elsewhere in this report, the Department should initiate a deeper evaluation of several key areas where strategic coordination is



especially important. Some of these evaluations are already underway; others will be part of the Department's ongoing efforts to evaluate its authorities, practices, and resources.

The eight non-exclusive areas for deeper evaluation include:

**1. *Strengthening Our Own Defenses:*** Consistent with the President's May 2017 Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure,<sup>16</sup> the Department is continually reassessing how best to defend its networks and reduce vulnerabilities. The Department should consider next steps and a longer-term strategy to maintain the security of its own defenses.

**2. *Enhancing Effective Collaboration with the Private Sector:*** The Department's ability to work collaboratively and effectively with the private sector will continue to be one of the most critical elements of our strategy to fight cybercrime. In the coming months, the Department should engage in a more extensive evaluation of our work with the private sector by seeking specific input from private sector participants. Where appropriate, we will make recommendations to enhance these collaborative efforts, including with regard to information-sharing, threat and incident notification, data breach notification standards, and frameworks for joint disruptive efforts, such as botnet take-downs.

**3. *Addressing Encryption and Anonymity (the Going Dark Array of Issues):*** Ad-

ressing the complex issues raised by the legal and technical barriers that prevent law enforcement from obtaining information in electronic form is another Department priority. As discussed above, it is critical that the Department maintain the ability to identify those who employ technology for illicit means and, with appropriate legal authority, to obtain evidence to bring criminals to justice. The Department should continue to develop a framework to ensure that these public safety and national security objectives can be met even as encryption and anonymizing technologies continue to evolve. In addition, the Department should explore and, as appropriate, adopt new investigative methods to replace the investigative opportunities that have been lost.

**4. *Addressing Malign Foreign Influence Operations:*** As discussed in Chapter 1, hostile foreign actors exploit the Internet and social media platforms to conduct influence operations against our Nation, including by spreading disinformation and propaganda online on a scale greater than has ever been observed before. In addition to implementing the disclosure policy discussed in Chapter 1, the Department should consider additional ways to improve our ability to respond to malign foreign influence operations, including whether new criminal statutes aimed directly at this threat are needed, and whether there are new ways we can work with the private sector in this area. Because this problem requires a whole-of-government solution, the Department should also consider how best to use existing or additional interagency coordination mechanisms to address the threat.

**5. Addressing the Global Nature of Cyber-Enabled Crime:** A hallmark of technology-enabled crime is that it increasingly cuts across international boundaries, even when less sophisticated actors are behind the malicious activity. As discussed above, the global nature of cybercrime carries with it numerous impediments—both technological and arising out of foreign laws and international agreements—to the Department’s ability to identify and locate malicious actors and bring them to justice. These impediments bear no easy solutions and may only grow as technology continues to evolve. The Department should continue evaluating this set of challenges and make additional recommendations to improve its global investigative and prosecutorial reach.

**6. Preparing for Emerging and Future Technology:** The technology behind current cyber-enabled threats will continue to evolve. The Department must ensure that its continued recalibration of efforts and resources not only aims at the major threats of today, but also prepares it for the emerging threats of tomorrow. The Department should continue to evaluate how its investigative and prosecutorial abilities can keep pace with, and even stay ahead of, the evolving technological threat. For example, the Department should continue evaluating the emerging threats posed by rapidly developing cryptocurrencies that malicious cyber actors often use, and autonomous vehicle technology, which has both ground and aerial applications (e.g., unmanned aircraft systems).

**7. Sharpening Departmental and Inter-agency Organization of Efforts to Fight Cyber-Enabled Crime:** The Department’s cyber-related mission requires effort and expertise from many components. Similarly, the Department’s efforts make up just one part of the U.S. government’s approach to cyber issues. As such, the Department must continuously review its internal coordination approach and resources, as well as how it interacts with its interagency partners, to determine if any improvements or adjustments are needed. Relatedly, the Department should continue evaluating how most effectively to recruit and retain attorneys, investigators, and professional staff with the necessary skills and mission-oriented mindset to ensure it has the human capital it needs to confront evolving cyber threats.

**8. Strengthening the Department’s Tools and Authorities:** This report has described numerous additional recommendations to strengthen the Department’s tools and authorities. Where such improvements are already known, the Department should seek ways to advance those improvements, including by seeking interagency approval to advocate for legislation, where appropriate.

In each of these key areas, the Department should not be merely reactive to known challenges and obstacles, but rather should pursue a strategic and forward-looking approach.



## NOTES

<sup>1</sup> Challenges specific to foreign influence operations are discussed in detail in Chapter 1 and so are not repeated here.

<sup>2</sup> The Digital Millennium Copyright Act, codified at 17 U.S.C. § 1201, prohibits the circumvention of technological controls, such as encryption and password protocols, that protect copyrighted works. Section 1201 also includes a rulemaking process that recognizes that, in some cases, exceptions to the general prohibition may be justified. Section 1201 requires the Copyright Office to conduct a rulemaking every three years to evaluate proposed exemptions proposed by the public to the anti-circumvention provision and to recommend appropriate proposals for adoption by the Librarian of Congress. The exemptions last only three years unless they are renewed in a subsequent proceeding.

<sup>3</sup> The last rulemaking process conducted in 2016 resulted, *inter alia*, in a three-year exemption for “security research” conducted on particular categories of devices, including machines designed for use by individual consumers, motorized land vehicles, and certain medical devices. Security research included “good faith testing for and the identification, disclosure and correction of malfunctions, security flaws and vulnerabilities in computer programs.” See generally U.S. COPYRIGHT OFFICE, “Section 1201 Rulemaking: Sixth Triennial Proceeding to Determine Exemptions to the Prohibition on Circumvention,” (Oct. 2015), available at: <https://www.copyright.gov/1201/2015/registers-recommendation.pdf> (last accessed June 29, 2018).

<sup>4</sup> See John T. Lynch, Jr., Chief, Department of Justice Computer Crime and Intellectual Property Section, to Regan Smith, General Counsel and Associate Register of Copyrights, Library of Con-

gress (June 28, 2018), available at: <https://www.justice.gov/criminal-ccips/page/file/1075496/download> (last accessed June 29, 2018). To date, the Department is unaware of any claims that the current security research exemption has thwarted or interfered with criminal investigations or prosecutions.

<sup>5</sup> Available at: <https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/04/30/04272015reporting-cyber-incidents-final.pdf> (last accessed June 29, 2018).

<sup>6</sup> See “Alabama Rolls with Tide as Last State to Adapt Breach Notification Law,” Taft Stettinius & Hollister LLP (Apr. 30, 2018), available at: <https://www.lexology.com/library/detail.aspx?g=cc0e9bb3-fe24-4211-b9dc-1fbfd350637f> (last accessed June 29, 2018).

<sup>7</sup> “Presidential Memorandum on the Actions by the United States Related to the Section 301 Investigation,” THE WHITE HOUSE (March 22, 2018), available at: <https://www.whitehouse.gov/presidential-actions/presidential-memorandum-actions-united-states-related-section-301-investigation/> (last accessed June 29, 2018).

<sup>8</sup> For example, due to such concerns, DHS in September 2017 issued a directive requiring federal agencies to remove and discontinue use of antivirus software provided by Moscow-based Kaspersky Lab. Several months later, Congress enacted a government-wide ban on Kaspersky products and services that exceeded the scope of the DHS prohibition. Both measures came in response to growing national security concerns presented by the presence of Kaspersky products on U.S. information systems. Kaspersky challenged both measures in court, and both suits

were dismissed at the pleading stage. Litigation continues in the court of appeals. Also in 2017, Congress amended 10 U.S.C. § 491 to restrict Department of Defense procurement of certain telecommunications equipment or services with particular Chinese or Russian origins.

<sup>9</sup> Accessing data is further complicated in some circumstances by the lack of any uniform data retention standards or requirements for service providers. Without such requirements, data that is potentially critical to law enforcement investigations is simply not retained or in some cases is not retained long enough to be useful.

<sup>10</sup> Telephone toll billing records include the originating phone number, the phone number called, and the date, time, and length of the call. ECTRs for e-mail show the sending e-mail address, the e-mail recipients, and the date, time, and size of the e-mail message.

<sup>11</sup> See, e.g., *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008) (holding that e-mail and Internet users have no reasonable expectation of privacy in to/from addresses of their messages or in IP addresses of websites visited).

<sup>12</sup> See also *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 207 (4th Cir. 2012) (“[W]e reject an interpretation of the CFAA that imposes liability on employees who violate a use policy[.]”); *United States v. Valle*, 807 F.3d 508 511 (2d Cir. 2015) (an individual “exceeds authorized access” only when he obtains or alters information that he does not have authorization

to access for any purpose which is located on a computer that he is otherwise authorized to access”).

<sup>13</sup> For instance, a criminal in one State can easily disseminate graphic images and personally-identifying information of his victim in another State or around the world. He can store the images and information on servers in unfriendly foreign jurisdictions, using proxy technology to conceal his true location. He can threaten and extort the victim using end-to-end encrypted communication applications that store little or no information about subscribers. Without leaving home, the perpetrator can commit an elaborate and hard-to-trace scheme using technology easily accessible to anyone. Worse, someone with no technical sophistication at all can hire someone to do the harassment for him from a dark market online.

<sup>14</sup> “A Report to the President on Enhancing the Resilience of the Internet and Communications Ecosystem Against Botnets and Other Automated, Distributed Threats,” U.S. DEPT. OF COMMERCE & U.S. DEPT. OF HOMELAND SECURITY (May 22, 2018), available at: [https://www.commerce.gov/sites/commerce.gov/files/media/files/2018/eo\\_13800\\_botnet\\_report\\_-\\_finalv2.pdf](https://www.commerce.gov/sites/commerce.gov/files/media/files/2018/eo_13800_botnet_report_-_finalv2.pdf) (last accessed June 29, 2018).

<sup>15</sup> 18 U.S.C. §§ 981-83.

<sup>16</sup> Exec. Order No. 13,800, 82 Fed. Reg. 22391 (May 16, 2017).









**Office of the Attorney General**

**Washington, D. C. 20530**

February 16, 2018

MEMORANDUM FOR HEADS OF DEPARTMENT COMPONENTS

FROM: THE ATTORNEY GENERAL

SUBJECT: Cyber-Digital Task Force

The malicious use of technology poses an unprecedented threat against our nation. While computers, smart devices, and other chip-enabled machines—as well as the networks that connect them—have enriched our lives and have driven our economy, the malign use of these technologies harms our government, victimizes consumers and businesses, and endangers public safety and national security. Indeed, the scale of this cyber threat, and the range of actors that use cyber intrusions and attacks to achieve their objectives, have grown in alarming ways.

The Department of Justice remains committed to confronting cyber threats by detecting, deterring, and disrupting malicious cyber activity through the enforcement of federal law. Therefore, today, I am establishing the Department's Cyber-Digital Task Force (the Task Force). This Task Force not only will canvass the many ways that the Department already combats the global cyber threat, but also will identify how federal law enforcement can more effectively accomplish its mission in this vital and evolving area.

The Task Force shall be chaired by a senior Department official appointed by the Deputy Attorney General and shall consist of representatives from the Criminal Division; the National Security Division; the United States Attorney's Office community; the Office of Legal Policy; the Office of Privacy and Civil Liberties; the Office of the Chief Information Officer; the Bureau of Alcohol, Tobacco, Firearms and Explosives; the Drug Enforcement Administration; the Federal Bureau of Investigation; and the United States Marshals Service. The Deputy Attorney General may invite representatives from other Department components, and from other federal agencies, to participate in the Task Force as appropriate, and may establish subcommittees to focus the Task Force's efforts.

Many of the most pressing cyber threats that our nation faces transcend easy categorization. These threats include: efforts to interfere with, or disable, our critical infrastructure; efforts to interfere with our elections; use of the Internet to spread violent ideologies and to recruit followers; theft of corporate, governmental, and private information on a mass scale; use of technology to avoid or frustrate law enforcement, or to mask criminal activity; and the mass exploitation of computers, along with the weaponizing of everyday consumer devices (as well as of the very architecture of the Internet itself) to launch attacks on American citizens and businesses. Evaluating these threats, and formulating a strategy to combat them, should be among the Task Force's highest priorities.

## CYBER-DIGITAL TASK FORCE REPORT

---

Memorandum for Heads of Department Components  
Subject: Cyber-Digital Task Force

Page 2

I have asked for an initial report from the Task Force describing the Department's current cyber-related activities and offering initial recommendations by no later than June 30, 2018.

The Internet has transformed our lives. We must ensure that Internet-based technologies remain sources of enrichment, rather than becoming forces of destruction and vectors of chaos. I look forward to our continued work together in support of a prosperous and safe America.

---

## APPENDIX 2

### RECENT SUCCESSFUL BOTNET DISRUPTIONS

#### *VPNFilter*

In May 2018, the Department took steps to disrupt the operation of a global botnet of hundreds of thousands of infected home and office (“SOHO”) routers and other networked devices under the control of a group of actors known as the “Sofacy Group” (also known as “apt28,” “sandworm,” “x-agent,” “pawn storm,” “fancy bear” and “sednit”).<sup>1</sup> The botnet, which the FBI and cybersecurity researchers called “VPNFilter,” targets SOHO routers and network-access storage devices. In order to identify infected devices and facilitate their remediation, the U.S. Attorney’s Office for the Western District of Pennsylvania applied for and obtained court orders authorizing the FBI to seize a domain that is part of the malware’s command-and-control infrastructure. The FBI also put out a public service announcement urging individuals and organizations to reset their routers.<sup>2</sup>

The cumulative effect of these actions would be to purge parts of the malware from the routers that were reset, and to direct attempts by the remaining malware to reinfect the device to an FBI-controlled server, which captured the Internet Protocol (“IP”) address of infected devices. A non-profit partner organization agreed to disseminate the IP addresses to those who can assist with remediating the botnet, including foreign CERTs and Internet service providers.

Although the devices would remain vulnerable to reinfection while connected to the Internet, these efforts maximized opportunities to identify and remediate the infection worldwide in the time available before Sofacy actors learned of the vulnerability in their command-and-control infrastructure.

#### *Kelihos*

On April 10, 2017, the Department announced an extensive effort to disrupt and dismantle the Kelihos botnet—a global network of tens of thousands of computers infected with the Kelihos malware.<sup>3</sup> Under the control of a cybercriminal, Peter Levashov, that botnet facilitated a range of malicious activities, including harvesting login credentials, distributing hundreds of millions of spam e-mails, and installing ransomware and other malicious software. The enormous volume of unsolicited spam e-mails sent by the botnet advertised counterfeit drugs, work-at-home scams, and a variety of other frauds, including deceptively promoted stocks in order to fraudulently increase their price (so-called “pump-and-dump” stock fraud schemes).

To liberate the victim computers from the botnet, the Department obtained civil and criminal court orders that authorized measures to neutralize the Kelihos botnet by (1) seizing domain names that the botnet used to communicate with the command-and-control servers, (2) establishing substitute servers that received the automated requests for instructions so that infected computers no longer communicated with the criminal operator, and (3) blocking any commands sent from the criminal operator attempting to regain control of the infected computers. As described in Chapter 3, Levashov was arrested in Spain and extradited to the U.S. to face justice.

#### *Avalanche*

On November 30, 2016, the Department, in coordination with German state and federal police, Europol, and various other countries and entities, conducted a takedown operation against



the Avalanche malware infrastructure. This takedown led to the disabling of seven botnets that relied on this infrastructure and impacted approximately 10 different malware families that had utilized the Avalanche network.

The Avalanche network offered cybercriminals a secure infrastructure, designed to stand in the way of detection by law enforcement and cyber security experts, over which the criminals conducted malware campaigns as well as money laundering schemes known as “money mule” schemes. Access to the Avalanche network was offered to the cybercriminals through postings on exclusive underground online criminal forums. In these schemes, highly organized networks of “mules” purchased goods with stolen funds, enabling cybercriminals to launder the money they acquired through malware attacks or other illegal means.

The types of malware and money mule schemes operating over this network varied. Ransomware, such as Nymain, encrypted victims’ computer files until the victim paid a ransom (typically in a form of electronic currency) to the cybercriminal. Other malware, such as GozNym, was designed to steal victims’ sensitive banking credentials, which were directed through the intricate network of Avalanche servers to backend servers controlled by the cybercriminals and used to initiate fraudulent wire transfers.

The Avalanche network, which had been operating since at least 2010, was estimated to involve hundreds of thousands of infected computers worldwide. The monetary losses associated with malware attacks conducted over the Avalanche network were estimated to be in the hundreds of millions of dollars worldwide, although exact calculations are difficult due to the high number of malware families present on the network.

This operation required an unprecedented level of international coordination to seize, block, and sinkhole over 800,000 malicious domains associated with the Avalanche network. These domains had been used to send commands to infected devices, pass banking credentials to cyber criminals, and obfuscate efforts by law enforcement to investigate this conspiracy. The USAO for the Western District of Pennsylvania and the Computer Crime and Intellectual Property Section obtained a temporary restraining order which greatly assisted in this effort. The Department continues to build on the success of this operation, using information obtained through seized infrastructure to identify and arrest criminals responsible for the creation of the malware distributed via Avalanche.

### *Gameover Zeus & Cryptolocker*

In 2014, the Department led a coalition of nearly a dozen foreign countries and a group of elite computer security firms to disrupt and dismantle the highly-sophisticated “Gameover Zeus botnet.”<sup>4</sup> At its peak, that botnet consisted of a global network of between 500,000 and 1 million computers infected malware that used keystroke logging to collect online financial account information and, in turn, inflicted more than \$100 million of losses to individuals in the United States. The Gameover Zeus network was also used to spread the Cryptolocker ransomware, which used cryptographic key pairs to encrypt the computer files of its victims and often left victims with no choice but to pay hundreds of dollars to obtain the decryption keys needed to unlock their files. As of April 2014, security researchers estimated that Cryptolocker had infected more than 234,000 computers and, according to one estimate, caused more than \$27 million in ransom payments in its first two months in circulation.



To disrupt both the Gameover Zeus botnet and the Cryptolocker malware, the Department deployed a combination of criminal and civil tools available to law enforcement. As an initial matter, a federal grand jury indicated a key administrator of the botnet (Evgeniy Bogachev) with a 14-count indictment, and the Department filed a separate civil injunction against Bogachev as the leader of a tightly-knit gang of cyber criminals based in Russia and Ukraine responsible for both the Gameover Zeus and Cryptolocker schemes. Further, as in *Kelihos*, the Department obtained civil and criminal court orders authorizing measures to redirect requests for instructions by computers victimized by the two schemes away from the criminal operators to substitute servers established pursuant to court order. The FBI was also authorized to obtain the IP addresses of the victim computers reaching out to the substitute servers, and to provide that information to DHS's Computer Emergency Readiness Team (US-CERT) to help victims remove the Gameover Zeus malware from their computers.<sup>5</sup>

To identify servers as command-and-control hubs for the Gameover Zeus botnet and Cryptolocker malware, and to subsequently facilitate victims' efforts to remediate the damage to their computers, the Department also enlisted the assistance of numerous computer security firms and leading universities.

### *Coreflood*

In 2011, the Department disrupted and disabled the decade-old "Coreflood" botnet through a civil complaint, search warrants, a criminal seizure warrant, and a temporary restraining order.<sup>6</sup>

This botnet was a global network of 100,000 computers infected with a particularly harmful type of malware named Coreflood, which could

be controlled remotely to steal private personal and financial information from unsuspecting computer users. The botnet's administrators, in turn, used the stolen information for a variety of criminal purposes, including stealing funds from the compromised accounts. In one example described in court filings, for instance, Coreflood leveraged information gleaned through illegal monitoring of Internet communications between a user and the user's bank to take over an online banking session and cause the fraudulent transfer of funds to a foreign account.

The Department employed a multi-prong enforcement strategy to dismantle the Coreflood botnet. It obtained search warrants to seize five command-and-control servers that remotely controlled hundreds of thousands of infected computers, and a seizure warrant to secure 29 domain names that the botnet used to communicate with the command-and-control servers. Federal authorities also obtained a temporary restraining order that authorized the government to replace the illegal command-and-control servers with substitute servers. To prevent the defendants from reconstituting the botnet through new servers, domains, and updated software, the TRO also authorized the government to respond to routine requests for direction from the infected computers in the United States with a command that temporarily stopped the Coreflood malware from running on the infected computers. By limiting the defendants' ability to control the botnet, computer security providers and victims were given the time and opportunity to remove the malware from infected computers. The Department also filed a civil complaint against 13 "John Doe" defendants associated with the botnet.

## NOTES

<sup>1</sup> Press Release, “Justice Department Announces Actions to Disrupt Advanced Persistent Threat 28 Botnet of Infected Routers and Network Storage Devices,” U.S. DEPT. OF JUSTICE (May 23, 2018), available at: <https://www.justice.gov/opa/pr/justice-department-announces-actions-disrupt-advanced-persistent-threat-28-botnet-infected> (last accessed June 29, 2018).

<sup>2</sup> FEDERAL BUREAU OF INVESTIGATION, “Foreign Cyber Actors Target Home and Office Routers and Networked Devices Worldwide” (May 25, 2018), available at: <https://www.ic3.gov/media/2018/180525.aspx> (last accessed June 29, 2018).

<sup>3</sup> Press Release, “Justice Department Announces Actions to Dismantle Kelihos Botnet,” U.S. DEPT. OF JUSTICE (Apr. 10, 2017), available at: <https://www.justice.gov/opa/pr/justice-department-announces-actions-dismantle-kelihos-botnet-0> (last accessed June 29, 2018).

<sup>4</sup> Press Release, “U.S. Leads Multi-National Action Against “Gameover Zeus” Botnet and “Cryptolocker” Ransomware, Charges Botnet Administrator,” U.S. DEPT. OF JUSTICE (June 2, 2014), available at: <https://www.justice.gov/opa/pr/us-leads-multi-national-action-against-gameover-zeus-botnet-and-cryptolocker-ransomware> (last accessed June 29, 2018).

<sup>5</sup> At no point during the operation did the FBI or law enforcement access the content of any of the victims’ computers or electronic communications.

<sup>6</sup> Press Release, “Department of Justice Takes Action to Disable International Botnet,” U.S. DEPT. OF JUSTICE (Apr. 13, 2011), available at: <https://www.justice.gov/opa/pr/department-justice-takes-action-disable-international-botnet> (last accessed June 29, 2018).

---

## APPENDIX 3

### RECENT SUCCESSFUL DARK WEB DISRUPTIONS

#### *AlphaBay & Hansa*

On July 20, 2017, the Department announced the seizure of AlphaBay, an online criminal marketplace that had operated for over two years on the dark web and facilitated the sale throughout the world of deadly illegal drugs, stolen and fraudulent identification documents and access devices, counterfeit goods, malware and other computer hacking tools, firearms, and toxic chemicals. Around the time of its takedown, AlphaBay was the largest criminal marketplace on the Internet. Indeed, prior to the site's disruption, one AlphaBay staff member claimed that it serviced over 200,000 users and 40,000 vendors. AlphaBay operated as a hidden service on the "Tor" network, and used cryptocurrencies including Bitcoin, Monero, and Ethereum in order to hide the locations of its underlying servers and the identities of its administrators, moderators, and users. Based on law enforcement's investigation of AlphaBay, authorities believe the site was also used to launder hundreds of millions of dollars deriving from illegal transactions on the website.

The operation to seize the AlphaBay site coincided with efforts by Dutch law enforcement to investigate and take down the Hansa Market, another prominent dark web market. Like AlphaBay, Hansa Market was used to facilitate the sale of illegal drugs, toxic chemicals, malware, counterfeit identification documents, and illegal services. To maximize the disruptive impact of the joint takedowns, Dutch authorities took covert control over the Hansa Market during the period when AlphaBay was shutdown. That covert control not only allowed Dutch police to identify and disrupt the regular criminal activity on Hansa, but then also allowed the authorities to

sweep up all those new users who were displaced from AlphaBay and needed a new trading platform. The success of this joint operation stands out as yet another example of what international law enforcement can accomplish when working closely together to neutralize a cybercrime marketplace.

#### *Silk Road*

In late 2013, the Department joined with various law enforcement partners across the government to disrupt the hidden "Silk Road" website, and to prosecute its creator and owner, Ross Ulbricht.<sup>1</sup>

For the two years leading up to the Department's actions, Silk Road stood out as the most sophisticated and extensive criminal marketplace on the Internet, serving as a sprawling black-market bazaar where unlawful goods and services, including illegal drugs of virtually all varieties, were regularly bought and sold. At its height, several thousand drug dealers and other unlawful vendors used the site to distribute hundreds of kilograms of illegal drugs and other unlawful goods and services to well over 100,000 buyers, and to launder hundreds of millions of dollars deriving from these unlawful transactions.

To remain outside the reach of law enforcement, Silk Road's administrators anonymized the site's transactions by operating it on the Tor network and including a Bitcoin-based payment system designed to conceal its users' identities and locations. Despite these efforts, law enforcement ultimately pierced Silk Road's cloak of anonymity and seized control of the website, its domain, its servers, and 29,655 Bitcoins residing on those servers (worth approximately \$28 million at the

time of seizure). The creator and administrator of Silk Road, Ross Ulbricht, was also arrested and ultimately convicted of seven charges relating to money laundering and computer hacking, among others, and sentenced to life in federal prison. The government seized an additional 144,336 Bitcoins from Ulbricht's computer hard drive (worth approximately \$130 million at the time of seizure).

### *Operation Onymous*

Building on the success of the Silk Road takedown, in November 2014, U.S. and European authorities took joint action against the underground website known as "Silk Road 2.0," as well as dozens of additional dark market websites that were facilitating the sale of an astonishing range of illegal goods and services on hidden services within the Tor network, including weapons, drugs, murder-for-hire services, stolen identification data, money laundering, hacking services, and others.<sup>2</sup> Silk Road 2.0 was created in November 2013 to fill the void left by the government's seizure of the Silk Road website in October 2013. As with Silk Road, the Department used civil forfeiture authorities to seize control over 400 Tor website addresses known as ".onion" addresses, as well as the servers hosting them. Adminis-

trators associated with these Dark Web markets were criminally prosecuted.

### *Darkode*

On July 15, 2015, the Department announced the dismantling of a computer hacking forum known as "Darkode" as part of a coordinated law enforcement action across 20 countries that led to the search, arrest, or charging of 70 Darkode members and associates.<sup>3</sup>

At the time of its takedown, the Darkode forum represented a uniquely grave threat to the integrity of data on computers because it provided a platform where highly-sophisticated cybercriminals congregated to buy, sell, and trade malware, botnets, and PII used to steal from U.S. citizens and individuals around the world. Before becoming a member of Darkode, prospective members were allegedly vetted through a process in which an existing member invited a prospective member to the forum for the purpose of presenting the skills or products that he or she could bring to the group. As part of Operation Shrouded Horizon, the FBI was able to disrupt and dismantle Darkode by infiltrating the forum's membership.



## NOTES

<sup>1</sup> Press Release, “Manhattan U.S. Attorney Announces Seizure of Additional \$28 Million Worth of Bitcoins Belonging to Ross William Ulbricht, Alleged Owner and Operator of “Silk Road” Website,” FEDERAL BUREAU OF INVESTIGATION (Oct. 25, 2013), available at: <https://archives.fbi.gov/archives/newyork/press-releases/2013/manhattan-u.s.-attorney-announces-seizure-of-additional-28-million-worth-of-bitcoins-belonging-to-ross-william-ulbricht-alleged-owner-and-operator-of-silk-road-website> (last accessed June 29, 2018).

<sup>2</sup> Press Release, “Dozens of Online ‘Dark Markets’ Seized Pursuant to Forfeiture Complaint Filed in Manhattan Federal Court in

Conjunction with the Arrest of the Operator of Silk Road 2.0,” FEDERAL BUREAU OF INVESTIGATION (Nov. 7, 2014), available at: <https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/dozens-of-online-dark-markets-seized-pursuant-to-forfeiture-complaint-filed-in-manhattan-federal-court-in-conjunction-with-the-arrest-of-the-operator-of-silk-road-2.0> (last accessed June 29, 2018).

<sup>3</sup> Press Release, “Major Computing Hacking Forum Dismantled,” U.S. DEPT. OF JUSTICE (July 15, 2015), available at: <https://www.justice.gov/opa/pr/major-computer-hacking-forum-dismantled> (last accessed June 29, 2018).



---

## APPENDIX 4

### GLOSSARY OF KEY TERMS

Acronym	Meaning
AECA	Arms Export Control Act
AUSA	Assistant United States Attorney
BEC	Business Email Compromise
Boyusec	Guangzhou Bo Yu Information Technology Company Limited
C&C	Command-and-Control
C.F.R.	Code of Federal Regulations
C2	Command and Control
CAATSA	Countering America's Adversaries Through Sanctions Act
CAN-SPAM	Controlling the Assault of Non-Solicited Pornography and Marketing
CAT	Cyber Action Team
CCIPS	Computer Crime and Intellectual Property Section
CFAA	Computer Fraud and Abuse Act
CHIP	Computer Hacking and Intellectual Property
CFIUS	Committee on Foreign Investment in the United States
CISO	Chief Information Security Officer
CLOUD	Clarifying Lawful Overseas Use of Data
CNN	Cable News Network
CTF	Cyber Task Force, Federal Bureau of Investigation
DDoS	Distributed Denial of Service
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DMCA	Digital Millennium Copyright Act
DOJ	Department of Justice
DSAC	Domestic Security Alliance Council

CYBER-DIGITAL TASK FORCE REPORT

Acronym	Meaning
EAR	Export Administration Regulations
ECPA	Electronic Communications Privacy Act
ECTR	Electronic Communication Transactional Record
EEA	Economic Espionage Act
EOUSA	Executive Office for United States Attorneys
ESU	Electronic Surveillance Unit
FBI	Federal Bureau of Investigation
FinCEN	Financial Crimes Enforcement Network
FISA	Foreign Intelligence Surveillance Act
FLASH	FBI Liaison Alert System
FSB	Russian Federal Security Service
GDPR	General Data Protection Regulation
HTOCU	Hi-Tech Organized Crime Unit
IC3	The Internet Crime Complaint Center
IEEPA	International Emergency Economic Powers Act
INTERPOL	International Criminal Police Organization
IoT	Internet of things
IP (address)	Internet Protocol
IPR	Intellectual Property Rights
IRS	Internal Revenue Service
ISIL	Islamic State of Iraq and the Levant
ISP	Internet Service Provider
JAR	Joint Analysis Report
J-CODE	Joint Criminal Opioid Darknet Enforcement
JITs	Joint Investigative Teams
JTA	Joint Technical Advisory
KAT	Kickass torrents



APPENDIX 4

Acronym	Meaning
<b>MLARS</b>	Money Laundering and Asset Recovery Section, Criminal Division
<b>MLAT</b>	Mutual Legal Assistance Treaty
<b>MUCD</b>	Military Unit Cover esignator
<b>NCCIC</b>	National Cybersecurity and Communications Integration Center
<b>NCFTA</b>	National Cyber-Forensics and Training Alliance
<b>NCIJTF</b>	National Cyber Investigative Joint Task Force
<b>NDCAC</b>	National Domestic Communications Assistance Center
<b>NICE</b>	National Initiative for Cybersecurity Education
<b>NITs</b>	Network Investigative Techniques
<b>NSCS</b>	National Security Cyber Specialists
<b>NSD</b>	National Security Division
<b>NSL</b>	National Security Letter
<b>OFAC</b>	Office of Foreign Assets Control
<b>OIA</b>	Office of International Affairs, Criminal Division
<b>OJT</b>	On the Job Training
<b>OLE</b>	Office of Legal Education
<b>P2P</b>	Peer-to-Peer
<b>PII</b>	Personally Identifiable Information
<b>PINs</b>	Private Industry Notifications
<b>PLA</b>	People's Liberation Army
<b>PPD</b>	Presidential Policy Directive
<b>PRC</b>	People's Republic of China
<b>PRTT</b>	Pen Register and Trap and Trace
<b>PSA</b>	Public Service Announcement
<b>RICO</b>	Racketeer Influenced and Corrupt Organizations Act
<b>ROB</b>	Rules of Behavior
<b>SCADA</b>	Supervisory Control and Data Acquisition

CYBER-DIGITAL TASK FORCE REPORT

---

Acronym	Meaning
<b>SPE</b>	Sony Pictures Entertainment
<b>STSO</b>	Operational Support Unit (Drug Enforcement Administration)
<b>SUA</b>	Specified Unlawful ctivity
<b>Tor</b>	The Onion Router
<b>TRO</b>	Temporary Restraining Order
<b>USAO</b>	United States ttorney's Office
<b>USNCB</b>	United States National Central Bureau (INTERPOL)
<b>US-CERT</b>	United States Computer Emergency Readiness Team
<b>USTR</b>	United States Trade Representative
<b>RRA</b>	Victims' Rights and Restitution ct
<b>WTI</b>	Workforce Training Initiative

## EXHIBIT 3

# Apple plasters privacy ad on billboard near Las Vegas Convention Center ahead of CES

By [AppleInsider Staff](#)

Friday, January 04, 2019, 06:44 pm PT (09:44 pm ET)

**Though Apple is not scheduled to make an appearance at the Consumer Electronics Show in Las Vegas next week, the company is using the event as an opportunity to push its message on privacy and has purchased a large billboard near the city's convention center.**



Source: [Chris Velazco](#) via [Twitter](#)

In an uncharacteristic move, Apple plastered a pithy ad touting the tenets of iPhone privacy on the side of a SpringHill Suites by Marriott hotel. The facility overlooks the Las Vegas Convention Center, where throngs of tech industry insiders will gather to network, take in keynote presentations and preview the latest and greatest gadgets.

Spotted by *Engadget* reporter [Chris Velazco](#) on [Friday](#), the black-and-white (but mostly black) ad reads, "What happens on your iPhone, stays on your iPhone." The line, a sendup of Las Vegas' own marketing catchphrase "What happens in Vegas, stays in Vegas," is accompanied by a line drawing of an iPhone XS and the address of Apple's [privacy webpage](#).

The billboard's location — standing tall over the heart of CES — is likely not a coincidence. Attendees will undoubtedly see the sign on their way to or from the event floor, where companies with less scrupulous privacy policies are set to show off their latest wares.

Apple typically refrains from participating in the CES hubbub in an official capacity, though "undercover" employees have been known to [prowl the grounds](#). Instead of taking part in major industry expos, the Cupertino tech giant relies on its own launch events and annual developers conference to shine a light on new products and services.

While Apple does not participate in CES festivities, its presence is nonetheless felt through the innumerable accessory makers building products that jibe with popular Apple devices like iPhone and Mac. Last CES saw a boom in HomeKit-compatible products, from light bulbs to obscure integrations like home shower systems.

*AppleInsider will be attending the Las Vegas Consumer Electronics Show starting on January 8 through January 11 where we're expecting 5G devices, HomeKit, 8K monitors and more. Keep up with our coverage by downloading the AppleInsider app, and follow us on YouTube, Twitter @appleinsider and Facebook for live, late-breaking coverage. You can also check out our official Instagram account for exclusive photos throughout the event.*



## EXHIBIT 4

## EXHIBIT 5

**O'Callaghan, Edward C. (ODAG)**

---

**From:** O'Callaghan, Edward C. (ODAG)  
**Sent:** Saturday, March 16, 2019 12:55 PM  
**To:** Rosenstein, Rod (ODAG)  
**Subject:** Fwd: (b)(3) [Fed. R. Crim. P. 6(e)] per EOUSA  
**Attachments:** (b)(3) [Fed. R. Crim. P. 6(e)] per EOUSA pdf; ATT00001.htm

Edward C. O'Callaghan

(b) (6)

Begin forwarded message:

**From:** "Khuzami, Robert (USANYS)" <(b) (6)>  
**To:** "Lan, Iris (ODAG)" <(b) (6)>, "O'Callaghan, Edward C. (ODAG)" <(b) (6)>  
**Subject:** (b)(3) [Fed. R. Crim. P. 6(e)] per EOUSA

Attached is the (b)(3) [Fed. R. Crim. P. 6(e)] per EOUSA which has attached to it the (b)(3) [Fed. R. Crim. P. 6(e)] per EOUSA

Rob

Begin forwarded message:

---

**From:** Rosenstein, Rod (ODAG)  
**Sent:** Friday, April 12, 2019 11:46 AM  
**To:** Peterson, Andrew (ODAG); Raman, Sujit (ODAG)  
**Cc:** O'Callaghan, Edward C. (ODAG); Ellis, Corey F. (ODAG)  
**Subject:** RE: Met club remarks  
**Attachments:** 4-12-19 DAG Metropolitan Club Remarks.Cyber.docx

Revised draft.

---

**From:** Peterson, Andrew (ODAG) (b) (6) >  
**Sent:** Monday, April 8, 2019 8:47 AM  
**To:** Rosenstein, Rod (ODAG) (b) (6) >  
**Cc:** O'Callaghan, Edward C. (ODAG) (b) (6) >; Ellis, Corey F. (ODAG) (b) (6) >  
**Subject:** FW: Met club remarks

Duplicative Information - See Document ID 0.7.22218.397295



---

**From:** Boyd, Stephen E. (OLA)  
**Sent:** Thursday, April 18, 2019 4:28 PM  
**To:** O'Callaghan, Edward C. (ODAG); Rosenstein, Rod (ODAG); Rabbitt, Brian (OAG); Lasseter, David F. (OLA)  
**Subject:** Hill Reax on SCO Report

Below: A recap of comments and statements made by key MOCs re: the Report. We'll do another survey tomorrow. SB

**Mitch McConnell – Senate Majority Leader**

**Mitch McConnell Press Release – [I Look Forward to Reviewing the Special Counsel's Report](#)**

"I'm grateful for the Attorney General's diligent work to release as much of the Special Counsel's report as possible to Congress and to the American people. The nation is fortunate to have an experienced leader like Bill Barr in place to ensure maximum possible transparency while carefully protecting classified material and legally restricted grand jury information. Like all of my colleagues, I look forward to carefully reviewing the report."

**Washington Post – [McConnell says Mueller investigation 'could not have been handled in a better way' \(Video\)](#)**

"Senate Majority Leader Mitch McConnell (R-Ky.) weighed in on special counsel Robert S. Mueller III's investigation following the release of the redacted report April 18."

**Chuck Schumer – Senate Minority Leader**

**Chuck Schumer and Nancy Pelosi Joint Press Release – [Leader Schumer And Speaker Pelosi Call For Special Counsel Mueller to Provide Public Testimony In House And Senate](#)**

"Attorney General Barr's regrettably partisan handling of the Mueller report, including his slanted March 24th summary letter, his irresponsible testimony before Congress last week, and his indefensible plan to spin the report in a press conference later this morning — hours before he allows the public or Congress to see it — have resulted in a crisis of confidence in his independence and impartiality. We believe the only way to begin restoring public trust in the handling of the Special Counsel's investigation is for Special Counsel Mueller himself to provide public testimony in the House and Senate as soon as possible. The American people deserve to hear the truth."

**[Chuck Schumer's Twitter](#)**

- 2:00 PM – "The differences are stark between what Attorney General Barr said on obstruction and what Special Counsel Mueller said on obstruction."
- 10:42 AM – As we continue to review the report, one thing is clear: Attorney General Barr presented a conclusion that the president did not obstruct justice while Mueller's report appears to undercut that finding."
- 7:12 AM – "Now that President @realDonaldTrump's campaign press conference is over:  
  
It's time for Congress and the American public to see the #MuellerReport."
- 6:10 AM – "AG Barr's handling of the #MuellerReport has been regrettably partisan, including his slanted 3/24 summary letter, irresponsible testimony before Congress, & indefensible plan to spin the report in a press conference today—hours before he allows the public or Congress to see it.

This has resulted in a crisis of confidence in AG Barr's independence & impartiality.

We believe the only way to begin restoring public trust in the handling of the Special Counsel's investigation is for Mueller himself to provide public testimony in the House & Senate ASAP.

The American people deserve to hear the truth."

- 4:05 AM – "We believe the only way to begin restoring public trust in the handling of the Special Counsel's investigation is for Special Counsel Mueller himself to provide public testimony in the House and Senate as soon as possible.

The American people deserve to hear the truth."

#### **Vox – [Nancy Pelosi and Chuck Schumer want Robert Mueller to testify to Congress](#)**

"Though Mueller did not make a determination on obstruction of justice, Barr himself, in coordination with Deputy Attorney General Rod Rosenstein, made a decision that the actions of the president did not qualify as criminal obstruction of justice.

Democrats are suspicious of Barr's decision on obstruction, especially because his report quoted Mueller saying, "while this report does not conclude that the President committed a crime, it also does not exonerate him." They now want to hear Mueller explain the report in his own words, rather than Barr's interpretation of them."

#### **The Hill – [Schumer slams Justice Dept over 'pre-damage control' on Mueller report](#)**

"Senate Minority Leader Chuck Schumer (D-N.Y.) ripped Attorney General William Barr over his plan to hold a press conference Thursday on special counsel Robert Mueller's final report before Congress has a chance to read the document.

"The American people deserve the truth," Schumer tweeted Wednesday. "They don't need any more pre-damage control or spin from [President Trump's] hand-picked attorney general, William Barr. Mr. Barr is acting more like a Trump campaign spokesman than an independent agent of the law."

#### **U.S. News – [Top Democrats Say Mueller Report Undercuts Barr Claims on Trump Obstruction](#)**

"The two top Democrats in Congress said on Thursday that Special Counsel Robert Mueller's report undercuts claims by Attorney General William Barr that President Donald Trump did not obstruct justice in the federal Russia probe."

#### **Kevin McCarthy – House Minority Leader**

##### **Kevin McCarthy Press Release – [Leader McCarthy Statement on Public Release of Mueller Report](#)**

"Nothing we saw today changes the underlying results of the 22-month long Mueller investigation that ultimately found no collusion.

Notwithstanding the partisan echo chamber to do otherwise, I fully approve of how Attorney General Barr has balanced legal requirements with the public's need to know in handling the release of the report. He complied with the law by protecting grand jury material, classified information, and the integrity of the investigative process. Democrats want to keep searching for imaginary evidence that supports their claims, but it is simply not there.

It is time to move on. Americans deserve better than this partisan quest to vilify a political opponent and I urge our Democratic colleagues in the House to put their emotions and opinions aside, and instead use that passion to come to the table and work on real solutions for all Americans."

#### **[Kevin McCarthy's Twitter](#)**

- 8:46 AM – "Democrats want to keep searching for imaginary evidence that supports their claims, but it is simply not there.

IT IS TIME TO MOVE ON.

Nothing we saw today changes the underlying results of the 22-month long Mueller investigation that ultimately found no collusion. I fully approve of how Attorney General Barr has balanced legal requirements with the public's need to know in handling the release of the report."

## Nancy Pelosi – Speaker of the House

### Nancy Pelosi and Chuck Schumer Joint Press Release – [Leader Schumer And Speaker Pelosi Call For Special Counsel Mueller to Provide Public Testimony In House And Senate](#)

“Attorney General Barr’s regrettably partisan handling of the Mueller report, including his slanted March 24th summary letter, his irresponsible testimony before Congress last week, and his indefensible plan to spin the report in a press conference later this morning — hours before he allows the public or Congress to see it — have resulted in a crisis of confidence in his independence and impartiality. We believe the only way to begin restoring public trust in the handling of the Special Counsel’s investigation is for Special Counsel Mueller himself to provide public testimony in the House and Senate as soon as possible. The American people deserve to hear the truth.”

#### [Nancy Pelosi’s Twitter](#)

2:00 PM – As we continue to review the report, one thing is clear: AG Barr presented a conclusion that @realDonaldTrump did not obstruct justice while the #MuellerReport appears to undercut that finding.”

- 11:04 AM – “The differences are stark between what Attorney General Barr said on obstruction and what Special Counsel Mueller said on obstruction. #MuellerReport
- 7:27 AM – “AG Barr has confirmed the staggering partisan effort by the Trump Admin to spin public’s view of the #MuellerReport – complete with acknowledgment that the Trump team received a sneak preview. It’s more urgent than ever that Special Counsel Mueller testify before Congress.”
- 4:36 AM – “Attorney General Barr’s partisan behavior has triggered a crisis of independence & impartiality.

The only way to begin restoring public trust in the handling of the Special Counsel’s investigation is for Special Counsel Mueller himself to provide public testimony in the House and Senate as soon as possible.”

### The Hill – [Top Democrats call for Mueller to publicly testify before Congress](#)

“Ahead of the release of a redacted version of the report on Thursday, House Speaker Nancy Pelosi and Senate Minority Leader Chuck Schumer broadly criticized Attorney General William Barr’s handling of the report, including his decision to hold a news conference to discuss it prior to its release to lawmakers and the American public.

Pelosi and Schumer accused Barr of creating “a crisis of confidence in his independence and impartiality” and said in a statement that public testimony from Mueller himself in both the House and the Senate is “the only way to begin restoring public trust.”

## Mark Meadows

#### [Mark Meadows’ Twitter](#)

- 10:56 AM – “Seeing more claims that because the President was unhappy about being investigated, he must be guilty. Hard to call this critique anything other than completely unserious. Would you be happy about being accused and subsequently investigated for a crime you did not commit?”
- 8:56 AM – “Reminder: today when you hear people seizing on the idea that Mueller didn’t “prove innocence,” remember—that was never Mueller’s job. Prosecutors do not set out to prove a negative. They look for evidence to establish a case. They didn’t have one. It was never there. It’s over.”
- 7:25 AM – “What you’re seeing is unprecedented desperation from the left. They went all in on a collusion conspiracy that never existed, didn’t get the result they wanted, and now they’re throwing manufactured controversies at the wall to see if anything sticks. It won’t work. #NoCollusion”

- 5:50 AM – “A good theme to look for in politics: ‘when you have the facts, pound the facts. When you don’t have the facts, pound the table.’

My Democrat colleagues are doing a lot of table pounding today. Because they don’t have the facts. There was no collusion. It’s over.”

**Washington Examiner – [Mueller conclusion produced 'unprecedented desperation from the left'](#)**

“Rep. Mark Meadows, R-N.C., a longtime ally of President Trump and critic of the Russian collusion investigation, tweeted Thursday that Democrats are now attempting to create controversies because the Mueller report did not find the president guilty of collusion.

What you're seeing is unprecedented desperation from the left,” Meadows tweeted. “They went all in on a collusion conspiracy that never existed, didn't get the result they wanted, and now they're throwing manufactured controversies at the wall to see if anything sticks. It won't work. #NoCollusion.

Meadows and Rep. Jim Jordan, R-Ohio, believe Trump and his campaign team were improperly and politically targeted by federal investigators.”

**Politico – [‘Game over’: Republicans rejoice after Mueller concludes](#)**

“Prosecutors have one job, and that’s to prosecute and indict,” Meadows said.. “And if Bob Mueller in two-and-a-half years of investigation — which includes both the FBI and special prosecutor’s time — doesn’t bring charges, I don’t know how much longer we need to be talking about collusion and obstruction.

Still, many Senate Republicans were less eager than their House counterparts to jump to conclusions about a report that was still damning for the president’s attempts to meddle in the Russia investigation. The majority of them said they were eager to review the report and were hopeful that when they did, it would validate the more reflexive statements by GOP lawmakers saying it’s already time to move on.”

**Lindsey Graham – Senate Judiciary Committee Chairman**

**[Lindsey Graham Press Release – Chairman Graham Statement on Receipt of Mueller Report](#)**

[“The Senate Judiciary Committee has received Special Counsel Mueller’s report. The committee’s review of the report is ongoing.](#)

[Once again, I applaud Attorney General Barr for his commitment to transparency and keeping the American people informed, consistent with the law and our national security interests.](#)

[“I look forward to hearing the Attorney General’s testimony before the Senate Judiciary Committee on May 1, 2019.”](#)

**The Hill – [Graham says he's 'not interested' in Mueller testifying](#)**

Sen. Lindsey Graham (R-S.C.), the chairman of the Senate Judiciary Committee, is dismissing calls for special counsel Robert Mueller to testify about his probe into the 2016 election.

Graham, who is currently on a congressional trip in Africa, told McClatchy on Thursday that he was "not interested" in having the former FBI director come speak before his panel.

“He’s done his job,” Graham said about Mueller. “I’m not going to retry the case.”

Graham, who has emerged as a close ally of President Trump's, is likely to face steep pressure to reverse course and call Mueller before his committee. Attorney General William Barr is set to testify before the panel early next month, and Graham is planning a separate probe into the 2016 election and the investigation into former Secretary of State Hillary Clinton's emails, as well as other Obama-era matters.

**Dianne Feinstein – Senate Judiciary Committee Ranking Member**



### Dianne Feinstein's Twitter

- 11:17 AM – “The Mueller report lays out not only how Russia interfered in the 2016 election, but also related activities carried out by Trump campaign officials. It also details many instances where President Trump tried to obstruct or stop the investigation.

Moving forward, Congress needs the unredacted report and underlying evidence, a commitment from AG Barr to not interfere with other ongoing investigations and a series of Judiciary Committee hearings. Congress must ensure actions like the report details are never repeated.”

- 11:17 AM – Regarding Russian interference in the 2016 election, the Mueller report provides a very thorough review not only of Russian actions, but also of related activities carried out by Trump campaign officials. The report presents a campaign that, in Mueller’s words, ‘expected it would benefit electorally from information stolen and released through Russian efforts.

Regarding obstruction of justice, the report lays out 10 instances where President Trump tried to obstruct the investigation. While some of President Trump’s actions were public, the report provides significant new details about his efforts to interfere in the investigation and his desire to protect himself. The report goes on to state that ‘...Congress may apply the obstruction laws to the President’s corrupt exercise of the powers of office...”

Moving forward, Congress should receive the unredacted report and underlying evidence as soon as possible. Also, Attorney General Barr must commit to not interfere with other investigations, including the 14 investigations mentioned in the report and all congressional reviews. Finally, I will ask Chairman Graham to hold hearings before the Judiciary Committee, including with Special Counsel Mueller. Congress has an obligation to ensure that activities like those laid out in this report are never repeated.”

### **Jerrold Nadler – House Judiciary Committee Chairman**

#### **Jerrold Nadler Press Release – [Chairman Nadler Statement on Redacted Mueller Report](#)**

“Even in its incomplete form, the Mueller report outlines disturbing evidence that President Trump engaged in obstruction of justice and other misconduct.

The report concluded there was ‘substantial evidence’ that President Trump attempted to prevent an investigation into his campaign and his own conduct. Contrary to the Attorney General’s statement this morning that the White House ‘fully cooperated’ with the investigation, the report makes clear that the President refused to be interviewed by the Special Counsel and refused to provide written answers to follow-up questions; and his associates destroyed evidence relevant to the Russia investigation.”

#### **Joint House Chairmen Press Release – [House Chairs Demand AG Barr Cancel Press Conference on Mueller Report](#)**

“Today, House Judiciary Committee Chairman Jerrold Nadler, Permanent Select Committee on Intelligence Chairman Adam B. Schiff, Committee on Oversight and Reform Chairman Elijah E. Cummings, Committee on Financial Services Chairwoman Maxine Waters, and Committee on Foreign Affairs Chairman Eliot L. Engel issued the following joint statement calling for Attorney General William Barr to cancel a press conference on Special Counsel Mueller’s report scheduled to take place before Congress is set to receive the report”

### Jerrold Nadler's Twitter

- 8:57 AM – “This is exactly why we need to hear directly from Special Counsel Mueller and receive the full, unredacted report with the underlying evidence.”
- 7:05 AM – “We cannot take Attorney General Barr's word for it. We must read the full Mueller report, and the underlying evidence. This is about transparency and ensuring accountability.”
- 7:03 AM – “It is clear Congress and the American people must hear from Special Counsel Robert Mueller in person to better understand his findings. We are now requesting Mueller to appear before @HouseJudiciary as soon as possible.”

**USA Today – [Top Democrat Jerrold Nadler says Mueller report shows why Congress needs to hear from him](#)**

"A top Democrat Thursday said the second page of special counsel Mueller's report shows why Congress needs to hear directly from Mueller and see the full evidence he considered.

Shortly after the redacted report was released, House Judiciary Committee Chairman Jerrold Nadler pointed to Mueller's statement that investigators were unable to clear the president of obstruction of justice.

"The evidence we obtained about the President's actions and intent presents difficult issues that prevent us from conclusively determining that no criminal conduct occurred," the report states."

**Fox News – [Nadler requests Mueller testify before House Judiciary Committee 'as soon as possible'](#)**

"House Judiciary Committee Chairman Jerrold Nadler on Thursday requested Special Counsel Robert Mueller appear before his committee "as soon as possible"—and no later than May 23.

Nadler's request came prior to the Justice Department's imminent release of Mueller's report to Nadler's committee, the Senate Judiciary Committee, and the American public."

**The Hill – [Nadler accuses Barr of 'unprecedented steps' to 'spin' Mueller report](#)**

"House Judiciary Committee Chairman Jerrold Nadler (D-N.Y.) on Wednesday tore into Attorney General William Barr, accusing him of "waging a media campaign on behalf of President Trump" ahead of the release of special counsel Robert Mueller's report.

Flanked by other Democratic members of the Judiciary committee, Nadler took aim at Barr over his decision to not hand the report over to Congress until after the attorney general holds a press conference on the topic. Nadler was also critical of Barr following a New York Times report that the Justice Department has briefed the White House on Mueller's findings."

**Roll Call – [Nadler to subpoena the unredacted Mueller report and underlying materials](#)**

"House Judiciary Chairman Jerrold Nadler is officially issuing a subpoena to obtain the full, unredacted report authored by special counsel Robert S. Mueller III, and the underlying materials used in his investigation.

Just a few hours after the Department of Justice released a redacted version of Mueller's report to Congress and the public, Nadler said he will issue a subpoena for the full report and investigatory materials. The Judiciary Committee had voted to authorize him to do so earlier this month, and the chairman had said he would if the Department of Justice declined to willingly provide the full report to Congress."

**Video on 4-17-19 – [Nadler Speaks Ahead of Mueller Report Release](#)**

**Video on 4-18-19 – [Press Conference On The Mueller Report](#)**

**Doug Collins – House Judiciary Committee Ranking Member**

**[Doug Collins Press Release – Collins statement on Mueller report release](#)**

["The special counsel's 22-month investigation found no Americans conspired with Russia to interfere in our elections and Democrats' accusations of criminal obstruction are unfounded. I look forward to examining the mountain of facts supporting the principal conclusions the attorney general and deputy attorney general shared last month: no collusion, no obstruction.](#)

[I am encouraged by the Democrats and Republicans who have expressed their faith in Special Counsel Mueller's integrity and ability. The attorney general has delivered more transparency than the regulations require, partnering with the special counsel's team to make necessary redactions to a report that he is sharing with Congress in good faith, not by mandate.](#)

[I am thankful to Attorney General Barr for sharing this report."](#)

## Doug Collins' Twitter

- 9:07 AM – “#TBT to that time when Democrats' bar for crying collusion was apparently much higher than it is now. Today, when Mueller says "no collusion," Democrats reply, "Thanks, but we'll keep looking." #MuellerReport”
- 8:49 AM – “My full statement on @TheJusticeDept’s release of the #MuellerReport →”
- 7:48 AM – “#TBT--> @RepJerryNadler insisted acting AG Whitaker ask the White House to assert executive privilege before testifying before our committee, but Democrats are now upset the WH took the opportunity to decline to assert privilege regarding the #MuellerReport.”
- 7:04 AM – “#TBT --> For context, the Obama Administration asserted executive privilege over email between Eric Holder and his own mother, but @realDonaldTrump invoked no executive privilege, in unprecedented transparency. The contrast is so clear that even Democrats should see it.”
- 6:56 AM – “No collusion. No obstruction. No OLC opinion on sitting presidents considered in these determinations. No executive privilege asserted. No redactions proposed or made by anyone outside DOJ. No one outside DOJ viewed unredacted report. No cover up when there’s nothing to cover up.”

## **The Hill – Judiciary Republican: Nadler 'only person trying to spin' Mueller report**

“Rep. Doug Collins (R-Ga.), the ranking Republican on the House Judiciary Committee, blasted the panel’s chairman, Rep. Jerrold Nadler (D-N.Y.), over his criticism of the rollout for special counsel Robert Mueller’s report.

Nadler and other top Democrats have excoriated Attorney General William Barr over his intention to hold a 9:30 a.m. press conference, saying he hopes to spin the report before Congress will receive a redacted version of Mueller’s final conclusions between 11 a.m. and noon Thursday.”

## **Richard Burr – Senate Select Committee on Intelligence Chairman**

### **Richard Burr Press Release – Burr Statement on Release of Mueller Report**

“I appreciate Attorney General Barr’s commitment to publicly releasing the full report, excepting material that would compromise intelligence sources and methods, ongoing DOJ prosecutions, or legally protected grand jury information. The American people have a right to review as much of the report as possible to understand the Special Counsel’s conclusions and the reasoning behind them.

“I am reviewing Special Counsel Mueller’s report carefully. Furthermore, I look forward to presenting the American people with an accounting of the facts the Committee has uncovered as we conclude our own investigation. It is my hope to release the first of our final reports in the coming weeks.”

### **Politico – Burr apparently fed info on FBI's Russia probe to White House, Mueller says**

“Senate Intelligence Chairman Richard Burr apparently supplied the White House counsel's office with information about FBI investigations into Russian interference in the 2016 election, according to a report from special counsel Robert Mueller that was made public on Thursday.

The report says that on March 9, 2017, then-FBI Director James Comey briefed Congressional leaders and intelligence committee heads on the ongoing investigation into Russian interference. That briefing included "an identification of the principal U.S. subjects of the investigation."

Burr (R-N.C.) then corresponded with the White House a week later about the Russia probes and the White House counsel's office "appears to have received information about the status of the FBI investigation," the special counsel report said.”

## **Mark Warner – Senate Select Committee on Intelligence Ranking Member**

### [Mark Warner's Twitter](#)

- 12:38 PM – Here's what I'll say about the redacted Mueller report. It is clear that AG Barr fundamentally mischaracterized its findings this morning. Congress needs to see the full, unredacted report, with all materials underlying its findings, and hear directly from the Special Counsel.

### **Adam Schiff – House Permanent Select Committee on Intelligence Chairman**

#### **Joint House Chairmen Press Release – [House Chairs Demand AG Barr Cancel Press Conference on Mueller Report](#)**

“Today, House Judiciary Committee Chairman Jerrold Nadler, Permanent Select Committee on Intelligence Chairman Adam B. Schiff, Committee on Oversight and Reform Chairman Elijah E. Cummings, Committee on Financial Services Chairwoman Maxine Waters, and Committee on Foreign Affairs Chairman Eliot L. Engel issued the following joint statement calling for Attorney General William Barr to cancel a press conference on Special Counsel Mueller’s report scheduled to take place before Congress is set to receive the report”

### [Adam Schiff's Twitter](#)

- 8:25 AM – “The House Intelligence Committee has formally invited Special Counsel Mueller to testify on the counterintelligence investigation.

After a two year investigation, the public deserves the facts, not Attorney General Barr’s political spin.”

#### **Roll Call – [House Democrats press on with investigations after Mueller report release](#)**

“And in a letter Thursday inviting the special counsel to testify before the House Intelligence Committee, Chairman Adam Schiff wrote that the panel must receive “comprehensive testimony” from Mueller “about the investigation’s full scope and areas of inquiry,” underlying evidence, and any completed and ongoing counterintelligence investigations stemming from his probe.”

#### **Letter 4-18-19 - [Testimony Request](#)**

### **Devin Nunes – House Permanent Select Committee on Intelligence Ranking Member**

#### **Washington Examiner – [Devin Nunes looking for 'some type of setup' in 3 areas of Mueller's report](#)**

“House Intelligence Committee ranking member Devin Nunes, R-Calif., said he will be looking for information on "some type of setup" on three subjects in special counsel Robert Mueller's final report.

During an interview with Fox News host Laura Ingraham on Tuesday, the California Republican cited former national security adviser Michael Flynn, Maltese professor Joseph Mifsud, and the infamous June 2016 Trump Tower meeting as the subjects of interest he hopes to see.

"What I'm going to be looking for is there's three specific areas where I think there was some type of setup involved," Nunes said.”

### **Elijah Cummings – House Oversight and Government Reform Committee Chairman**

#### **Elijah Cummings Press Release – [Chairman Cummings Issues Statement on Mueller Report](#)**

“The President and his Attorney General expect the American people to be blind to what we can now see. This report catalogues in excruciating detail a proliferation of lies by the President to the American people, as well as his incessant and repeated efforts to encourage others to lie. Contrary to Attorney General Barr’s attempts at misdirection, it is crystal clear from the report that the Justice Department’s policy against indicting a sitting President played a key role in Special Counsel Mueller’s analysis—in fact, it is the very first point in the obstruction section of his report. Unfortunately, we still have only part of the story, and Congress must subpoena the full report and all underlying documents.

In the report released today, Special Counsel Mueller wrote: “The conclusion that Congress may apply the obstruction laws to the President’s corrupt exercise of the powers of the office accords with our constitutional system of checks and balances and the principle that no person is above the law.”

#### **Joint House Chairmen Press Release – [House Chairs Demand AG Barr Cancel Press Conference on Mueller Report](#)**

“Today, House Judiciary Committee Chairman Jerrold Nadler, Permanent Select Committee on Intelligence Chairman Adam B. Schiff, Committee on Oversight and Reform Chairman Elijah E. Cummings, Committee on Financial Services Chairwoman Maxine Waters, and Committee on Foreign Affairs Chairman Eliot L. Engel issued the following joint statement calling for Attorney General William Barr to cancel a press conference on Special Counsel Mueller’s report scheduled to take place before Congress is set to receive the report”

#### **[Elijah Cummings’ Twitter](#)**

- 11:37 AM – “The President and his Attorney General expect the American people to be blind to what we can now see.

This report catalogues in excruciating detail a proliferation of lies by the President to the American people, as well as his incessant and repeated efforts to encourage others to lie.

Contrary to AG Barr’s attempts at misdirection, it is crystal clear from the report that DOJ’s policy against indicting a sitting President played a key role in Special Counsel Mueller’s analysis—in fact, it is the very first point in the obstruction section of his report.

Unfortunately, we still have only part of the story, and Congress must subpoena the full report and all underlying documents.”

#### **Jim Jordan – House Oversight and Government Reform Committee Ranking Member**

#### **Ranking Member Jim Jordan Press Release – [RANKING MEMBER JIM JORDAN’S STATEMENT ON THE MUELLER REPORT](#)**

“Democrat Members of Congress should take a deep breath and read the Special Counsel’s report before jumping to conclusions. The Attorney General already confirmed what we long suspected. No collusion. No obstruction. It would be a miscarriage of justice to use cherry-picked bits of information from the report to sow further divisiveness and spread conspiracies that serve only to undermine our democratic institutions.

One thing, however, is clear with the release of the report today: this sad chapter of American history is behind us. It is time to turn back to the people’s work of improving the efficiency, economy, and effectiveness of how their tax dollars are spent.

Despite the Special Counsel’s findings, it seems nothing will stop Democrats in Congress from trying to get the President at all costs. We just learned this week that they have Memoranda of Understanding to coordinate their attacks. It would be a shame for the onslaught of misguided politicized investigations to continue. The American people expect more from those who represent them in Washington.”

#### **[Jim Jordan’s Twitter](#)**

- 9:06 AM – “Democrat members of Congress should take a deep breath and read the Special Counsel’s report before jumping to conclusions.

The Attorney General concluded what we long suspected. No collusion. No obstruction.

It would be a miscarriage of justice to use cherry-picked bits of information from the report to sow further divisiveness and spread conspiracies that serve only to undermine our democratic institutions.

One thing, however, is clear with the release of the report today: this sad chapter of American history is behind us.

It’s time to turn back to the people’s work of improving the efficiency, economy, and effectiveness of how their tax dollars are spent.



Despite the Special Counsel's findings, it seems nothing will stop Democrats in Congress from trying to get the President at all costs.

We just learned this week that they have Memoranda of Understanding to coordinate their attacks.

It would be a shame for the onslaught of misguided politicized investigations to continue.

The American people expect more from those who represent them in Washington."

- 7:03 AM – 'No collusion! No obstruction! Complete cooperation from the President. No executive privilege asserted.'

**Gary Peters – Senate Homeland Security and Governmental Affairs Committee Ranking Member**

[Gary Peters' Twitter](#)

- 12:25 PM "Read my statement on the release of the Mueller Report"

'After the Mueller investigation led to 200 criminal charges, dozens of indictments and more than half a dozen guilty pleas, it's well past time for the American people to see the Special Counsel's report. I've said consistently that the report should be made public so the American people have the facts regarding Russia's efforts to interfere in our democracy and can draw their own conclusions. I also believe that Special Counsel Mueller should testify publicly. In the meantime, I will review the report carefully and look closely at what is included and what is withheld in its release.'

**Stephen E. Boyd**  
Assistant Attorney General  
U.S. Department of Justice  
Washington, D.C.

(b) (6)

---

**From:** Rosenstein, Rod (ODAG)  
**Sent:** Thursday, April 25, 2019 12:03 PM  
**To:** Sutton, Sarah E. (OPA); Hovakimian, Patrick (ODAG); Stafford, Steven (OPA)  
**Cc:** Edward C O'Callaghan (b) (6); Corey F. Ellis (ODAG)  
(b) (6); Peterson, Andrew (ODAG)  
**Subject:** Draft for Armenian Bar tonight  
**Attachments:** 2019.04.25.Armenian.Bar.Award.docx

---

**From:** Davis, Katherine (b) (6) >  
**Sent:** Thursday, April 25, 2019 9:58 PM  
**To:** Rosenstein, Rod (ODAG)  
**Subject:** Fwd: DEPUTY ATTORNEY GENERAL ROD J. ROSENSTEIN DELIVERS REMARKS AT THE ARMENIAN BAR ASSOCIATION'S PUBLIC SERVANTS DINNER

So that happened!! Holy moly.

You are telling the story in your speech but you need to tell it to us.

Btw. Love the Armenian stories. Sounds like flying LOT Airlines in the 80's

Katherine Davis  
Producer, 60 Minutes  
CBS News  
524 West 57th Street  
New York, NY 10019

(b) (6)

(b) (6)

(b) (6)

Begin forwarded message:

**From:** "USDOJ-Office of Public Affairs" <[USDOJ-OfficeofPublicAffairs@public.govdelivery.com](mailto:USDOJ-OfficeofPublicAffairs@public.govdelivery.com)>  
**Date:** April 25, 2019 at 9:40:07 PM EDT  
**To:** (b)(6) Katherine Davis  
**Subject:** DEPUTY ATTORNEY GENERAL ROD J. ROSENSTEIN DELIVERS REMARKS AT THE ARMENIAN BAR ASSOCIATION'S PUBLIC SERVANTS DINNER  
**Reply-To:** [USDOJ-OfficeofPublicAffairs@public.govdelivery.com](mailto:USDOJ-OfficeofPublicAffairs@public.govdelivery.com)

External Email >

"Peri yerego." Good evening. Rick, I am grateful for your friendship and for your 20 years of exceptional service to the Department of Justi

[https://urldefense.proofpoint.com/v2/url?u=http-3A\\_\\_links.govdelivery.com-3A80\\_track-3Ftype-3Dclick-26enid-3DZWfzPTEmbWFpbGluZ2lkPTlwMTkwNDI2LjUxNzU2MTEmbWVzc2FnZWlkPU1EQi1QUkQtQlVM](https://urldefense.proofpoint.com/v2/url?u=http-3A__links.govdelivery.com-3A80_track-3Ftype-3Dclick-26enid-3DZWfzPTEmbWFpbGluZ2lkPTlwMTkwNDI2LjUxNzU2MTEmbWVzc2FnZWlkPU1EQi1QUkQtQlVMLTlwMTkwNDI2LjUxNzU2MTEmbWVzc2FnZWlkPU1EQi1QUkQtQlVMLTlwMTkwNDI2LjUxNzU2MTEmbWVzc2FnZWlkPU1EQi1QUkQtQlVM)  
LTlwMTkwNDI2LjUxNzU2MTEmbWVzc2FnZWlkPU1EQi1QUkQtQlVM  
GIkPWRhdmlza0BjYnNuZXdzLmNvbSZ1c2VyaWQ9ZGF2aXNrQGNic25ld3MuY29tJmZsPSZleHRyY

T1NdWx0aXZhcmlhdGVJZD0mJiY-3D-26-26-26100-26-26-26https-3A\_\_www.justice.gov\_-3Futm-5Fmedium-3Demail-26utm-5Fsource-3Dgovdelivery&d=DwMFAA&c=jGUuvAdBXp\_VqQ6t0yah2g&r=zQ4mXH3XUhU8f10eNd-\_iyesySBlcVPI3FmNYkvjd6s&m=ZRT6-5tnTUkmJu7n8NQtpTKpFrDJWExFM5iGrSKip64&s=OwH9m8KjbGiE3xFSiwSKv5R9xhypCX7T\_ar86Cltsdo&e=  
[REDACTED]

THURSDAY APRIL 27, 2019

## **DEPUTY ATTORNEY GENERAL ROD J. ROSENSTEIN DELIVERS REMARKS AT THE ARMENIAN BAR ASSOCIATION'S PUBLIC SERVANTS DINNER**

**New York, New York**

***Remarks as prepared for delivery***

"Peri yerego." Good evening.

Rick, I am grateful for your friendship and for your 20 years of exceptional service to the Department of Justice — including seven years as the United States Attorney for Northern New York.

I am pleased to see several U.S. Attorneys here tonight: Geoff Berman from Southern New York, Richard Donoghue from Eastern New York, Grant Jaquith from Northern New York, and Craig Carpenito from New Jersey; as well as eight former U.S. Attorneys, and many other current and former government employees.

I am thankful to Armenian Bar Association Chair Gerard Kassabian, and Vice Chairs Kathryn Ossian and Lucy Varpetian.

My wife served on your board of governors from 1993 to 2002. I got to know many of the members, particularly the group that traveled with us to Armenia in 1994 to celebrate the 75th anniversary of the University of Yerevan.

When I met Lisa in 1988, some of her relatives viewed me as "odan," an outsider to the culture. But recently a friend introduced me as "Armenian by Choice." After tonight, I have an even stronger claim to be an honorary Armenian.

"Shot Shenorhagal em." Thank you very much.

Our wedding featured an Armenian opera singer who is in the audience tonight, Maro Partamian. One of my favorite songs was “Lerner Hyreni,” or “Mountains of Armenia.” We hired the “Dark Eyes” band to play at the reception, which was great except that I chose a country song called “I Swear” by John Michael Montgomery for the first dance. It did not sound quite right with an Armenian accent.

One of Lisa’s relatives was raised in Syria, where government service was not highly valued. Before he approved of the marriage, he wanted to know when I planned to get a real job, in the private sector.

Unfortunately, many native-born Americans also are skeptical about government service. My Uncle Harold was a self-employed carpet installer. One beautiful spring afternoon in 1994, I called him from an office in the Department of Justice headquarters building. It was a Saturday. And when I told him that I was working through the weekend, he said, “I’m sorry to hear that.”

And I said, “You don’t understand. There is no place that I would rather be.”

I first walked into that building as a federal prosecutor on December 3, 1990, at age 25. I remember how honored I felt to represent the people of the United States. I will still feel the same way when I walk out for the last time next month.

I joined the Department of Justice because I believe in the mission. I stayed because I believe in the people who carry out the mission.

Our agents, analysts, and attorneys demonstrate great intellect and integrity. They possess superb academic credentials and exceptional character. They pass rigorous screening interviews and face thorough background checks every few years. They are ethical, honorable, and admirable people.

No organization with 115,000 employees is error-free. But we have serious, professional, nonpartisan internal watchdogs. We investigate credible misconduct allegations. We correct mistakes and punish wrongdoers.

I have served under five Presidents and nine Senate-confirmed Attorneys General — ten, if you count Bill Barr twice. I served mostly outside the D.C. beltway, but I worked at Department of Justice headquarters three times — four years in the early 1990s as a career prosecutor, four years in the early 2000s as a supervisor, and two years in my current job.

Our headquarters is a beautiful Depression-era building. I frequently speak about the inspiration that I draw from three aspects of the building – the art it contains; the people it employs; and the principles it represents.

There are reminders of heroes, mentors, and friends on every floor. They taught me that our Department stands for the principle that every American deserves the protection of the rule of law.

We use the term “rule of law” to describe our obligation to follow neutral principles. As President Trump pointed out, “we govern ourselves in accordance with the rule of law rather [than] ... the whims of an elite few or the dictates of collective will.”

Justice Anthony Kennedy explained it this way: in a rule of law system, when you apply to a government clerk for a permit and you satisfy the objective criteria, you are not asking for a favor. You are entitled to the permit, and it is the clerk’s duty to give it to you.



The idea that the government works for the people is relatively novel. In some countries, that concept of a government bound by law to serve the people does not exist.

When I visited Armenia in 1994, the nation was emerging from seven decades of Soviet domination. Gyumri and other northern cities were not yet rebuilt after the 1988 earthquake. The six-year war with Azerbaijan was halted by a recent ceasefire, but the blockade over Nagorno-Karabakh crippled the economy.

We flew on Air Armenia, which used a shabby old Russian jet. Our plane needed to stop for fuel in Bulgaria, and we heard that the pilots paid with cash.

Armenia faced many challenges in 1994. Many skilled and educated people had left the country. When we hired a taxi to visit Lake Sevan, the driver turned off the engine at every downhill stretch to conserve gasoline.

We stayed at a nice hotel near Republic Square, but some mornings there was no water to flush the toilets, and some evenings there was no electricity to cook the food.

I gave a lecture at the University of Yerevan about public corruption. When I finished, a student raised his hand. He asked, "If you can't pay bribes in America, then how do you get electricity?"

I repeat that question in many speeches. It usually elicits laughter. But the point is profound.

The question illustrates how that young man understood Soviet society. Corruption undermines law. It stifles innovation, creates inefficiency, and inculcates distrust.

The question explains why I devoted my career to law enforcement: because the rule of law is the foundation of human liberty. The rule of law secures our freedom. It will secure our children's freedom. And we can only achieve it if people who enforce the law set aside partisanship, because the rule of law requires a fair and independent process; a process where all citizens are equal in the eyes of the government.

I do not care how police officers, prosecutors, and judges vote, just as I do not care how soldiers and sailors vote. That is none of my business. I only care whether they understand that when they are on duty, their job is about law and not politics.

There is not Republican justice and Democrat justice. There is only justice and injustice.

In the courtyard of the Department of Justice headquarters, there is an inscription that reads, in Latin: "Privilegium Obligatio." It means that when you accept a privilege, you incur an obligation. Working for Justice is a privilege.

Our commensurate obligations are established by our oath to well and faithfully execute the duties of the office. To honor that oath, you need to know your office's unique duties. At our Department, our job is to seek the truth, apply the law, follow the Department's policies, and respect its principles.

The rule of law is our most important principle. Patriots must always defend the rule of law. Even when it is not in their personal interest, it is always in the national interest. If you find yourself asking, "What will this decision mean for me?" then you probably are not complying with your oath of office.

At my confirmation hearing in March 2017, a Republican Senator asked me to make a commitment. He said: “You’re going to be in charge of this [Russia] investigation. I want you to look me in the eye and tell me that you’ll do it right, that you’ll take it to its conclusion and you’ll report [your results] to the American people.”

I did pledge to do it right and take it to the appropriate conclusion. I did not promise to report all results to the public, because grand jury investigations are ex parte proceedings. It is not our job to render conclusive factual findings. We just decide whether it is appropriate to file criminal charges.

Some critical decisions about the Russia investigation were made before I got there. The previous Administration chose not to publicize the full story about Russian computer hackers and social media trolls, and how they relate to a broader strategy to undermine America. The FBI disclosed classified evidence about the investigation to ranking legislators and their staffers. Someone selectively leaked details to the news media. The FBI Director announced at a congressional hearing that there was a counterintelligence investigation that might result in criminal charges. Then the former FBI Director alleged that the President pressured him to close the investigation, and the President denied that the conversation occurred.

So that happened.

There is a story about firefighters who found a man on a burning bed. When they asked how the fire started, he replied, “I don’t know. It was on fire when I lay down on it.” I know the feeling.

But the bottom line is, there was overwhelming evidence that Russian operatives hacked American computers and defrauded American citizens, and that is only the tip of the iceberg of a comprehensive Russian strategy to influence elections, promote social discord, and undermine America, just like they do in many other countries.

In 1941, as Hitler sought to enslave Europe and Japan’s emperor prepared to attack America, Attorney General Robert Jackson admonished federal prosecutors about their role in protecting national security. He said: “Defense is not only a matter of battleships and tanks, of guns and [soldiers].... It is raw materials, machines and [people who] work in factories. It is public morale. It is a law abiding population and a nation free from internal disorder . . . the ramparts we watch are not only those on the outer borders which are largely the concern of the military services. There are also the inner ramparts of our society — the Constitution, its guarantees, our freedoms and the supremacy of law. These are yours to guard and their protection is your defense program.”

As acting Attorney General, it was my responsibility to make sure that the Department of Justice would do what the American people pay us to do: conduct an independent investigation; complete it expeditiously; hold perpetrators accountable if warranted; and work with partner agencies to counter foreign agents and deter crimes.

Today, our nation is safer, elections are more secure, and citizens are better informed about covert foreign influence schemes.

But not everybody was happy with my decision, in case you did not notice.

It is important to keep a sense of humor in Washington. You just need to accept that politicians need to evaluate everything in terms of the immediate political impact.

Then there are the mercenary critics, who get paid to express passionate opinions about any topic, often with little or no information. They do not just express disagreement. They launch ad hominem attacks unrestricted by truth or morality. They make threats, spread fake stories, and even attack your relatives. I saw one of the professional provocateurs at a holiday party. He said, "I'm sorry that I'm making your life miserable." And I said, "You do your job, and I'll do mine."

His job is to entertain and motivate partisans, so he can keep making money. My job is to enforce the law in a non-partisan way; that is the whole point of the oath of office.

In our Department, we disregard the mercenary critics and focus on the things that matter. As Goethe said, "Things that matter most must never be at the mercy of things that matter least." A republic that endures is not governed by the news cycle. Some of the nonsense that passes for breaking news today would not be worth the paper was printed on, if anybody bothered to print it. It quickly fades away. The principles are what abide.

America's founders understood that the rule of law is not partisan. In 1770, five American colonists died after British soldiers fired on a crowd in the Boston Massacre. The soldiers were charged with murder. Many people believed that they deserved the death penalty.

John Adams agreed to represent the soldiers. His political beliefs were firmly against them. But Adams felt obligated to protect their rights under the law.

Defending British soldiers was a very unpopular cause, to put it mildly. Adams faced a serious risk, in his words, of "infamy," or even "death." In a diary entry about the trial, he wrote as follows: "In the evening I expressed to Mrs. Adams all my apprehensions: That excellent Lady, who has always encouraged me, burst into ... Tears.... [S]he was very sensible of all the danger to her and to our children as well as to me, but she thought I had done as I ought, [and] she was ... willing to share in all that was to come and place her trust in Providence."

The rhetoric mirrors an earlier letter that Adams wrote to explain his preference for integrity over acclaim. Adams wrote that in theaters "the applause of the audience is of more importance to the actors than their own approbation. But upon the stage of life, while conscience claps, let the world hiss."

Adams endured harsh criticism in the court of public opinion. But in the court of law, he secured the acquittal of the British captain and six soldiers.

At the trial, Adams delivered a timeless tribute to the rule of law. He said that "[f]acts are stubborn things; and whatever may be our wishes, our inclinations, or the dictates of our passions, they cannot alter the state of facts and evidence."

Adams' words remind us that people who seek the truth need to avoid confirmation bias. Truth is about solid evidence, not strong opinions. A 19th century Philadelphia doctor remarked that "sincerity of belief is not the test of truth." Many people passionately believe things that are not true.

I spent most of my career prosecuting cases in federal courthouses. My past trials in courts of law contrast with my recent tribulations in the halls of Congress, the channels of cable television, and the pages of the internet.

The difference is in the standard of proof. In my business, we need to prove facts with credible evidence, prove them beyond any reasonable doubt, and prove them to the unanimous satisfaction of a neutral judge and an unbiased jury of 12 random citizens.

Pursuing truth requires keeping an open mind, avoiding confirmation bias, and always yielding to credible evidence. Truth may not match our preconceptions. Truth may not satisfy our hopes. But truth is the foundation of the rule of law.

If lawyers cannot prove our case in court, then what we believe is irrelevant.

But in politics, belief is the whole ball game. In politics – as in journalism – the rules of evidence do not apply. That is not a critique. It is just an observation.

Last year, a congressman explained why he decided not to run for reelection. He said, “I like ... job[s] where facts matter. I like jobs where fairness matters. I like jobs where, frankly, ... the process matters.”

He was describing an American courtroom. “I like the art of persuasion,” he said. “I like finding 12 people who have not already made up their minds and ... may [let] the facts prevail. That’s not where we are in politics.”

That congressman spoke the truth. It may never be where we are in politics. But it must always be where we are in law.

Attorney General Jackson spoke about the fiduciary duty of government lawyers, the obligation to serve as a trustee for the public interest. He contrasted the special duties of government lawyers with what he called “the volatile values of politics.” That was in 1940.

Jackson understood that “lawyers must at times risk ourselves and our records to defend our legal processes from discredit, and to maintain a dispassionate, disinterested, and impartial enforcement of the law.”

“We must have the courage to face any temporary criticism,” Jackson urged, because “the moral authority of our legal process” depends on the commitment of government lawyers to act impartially.

Jackson also spoke about the role of lawyers in preserving liberty. He used a parable about three stonecutters asked to describe what they are doing. The first stonecutter focuses on how the job benefits him. He says, “I am earning a living.” The second narrowly describes his personal task: “I am cutting stone.” The third man has a very different perspective. His face lights up as he explains what the work means to others: “I am helping to build a cathedral.”

“[W]hether we are aware of it or not,” Jackson explained, lawyers “do more than earn [a] living[]; we do more than [litigate] [individual] cases. We are building the legal structure that will protect ... human liberty” for centuries to come.

As my time in public service comes to an end, I encourage each of you to remember the cathedral. You are always building a legacy. You set an example for your colleagues, and you lay a foundation for your successors.





This email was sent to (b)(6) Katherine Davis using GovDelivery, on behalf of [U.S. Department of Justice Office of Public Affairs](#) · 950 Pennsylvania Ave., NW · Washington, DC 20530 · 202-514-2007 · TTY (866) 544-5309. GovDelivery may not use your subscription information for any other purposes. [Click here to unsubscribe.](#)

http://links.govdelivery.com:80/track?enid=ZWFzPTEmbWFPbGluZ2lkPTlwMTkwNDI2LjUxNzU2MTEmbWVzc2FnZWlkPU1EQi1QUkQtQlVMLTIwMTkwNDI2LjUxNzU2MTEmZGF0YWJhc2VpZD0xMDAxJnR5cGU9b3B1biZzZXJpYWw9MTc0NjQzNjAmZW1haWxpZD1kYXZpc2tAY2JzbnV3cy5jb20mdXNlcmIkPW RhdmIza0BjYnNuZXdzLmNvbSZmbD0mZXh0cmE9TXVsdGI2YXJpYXRISWQ9JiYm

---

**From:** Rosenstein, Rod (ODAG)  
**Sent:** Friday, April 26, 2019 12:02 AM  
**To:** Thiemann, Robyn L (DEA)  
**Subject:** Re: DEPUTY ATTORNEY GENERAL ROD J. ROSENSTEIN DELIVERS REMARKS AT THE ARMENIAN BAR ASSOCIATION'S PUBLIC SERVANTS DINNER

Thank you!

Sent from my iPhone

On Apr 25, 2019, at 9:57 PM, Thiemann, Robyn L (b)(6), (b)(7)(C) per DEA > wrote:

Fantastic speech, boss.

: )

Begin forwarded message:

**From:** USDOJ-Office of Public Affairs <[USDOJ-OfficeofPublicAffairs@public.govdelivery.com](mailto:USDOJ-OfficeofPublicAffairs@public.govdelivery.com)>  
**Date:** April 25, 2019 at 9:40:08 PM EDT  
**To:** (b)(6), (b)(7)(C) per DEA (Robyn Thiemann) >  
**Subject:** DEPUTY ATTORNEY GENERAL ROD J. ROSENSTEIN DELIVERS REMARKS AT THE ARMENIAN BAR ASSOCIATION'S PUBLIC SERVANTS DINNER  
**Reply-To:** <[USDOJ-OfficeofPublicAffairs@public.govdelivery.com](mailto:USDOJ-OfficeofPublicAffairs@public.govdelivery.com)>

"Peri yerego." Good evening. Rick, I am grateful for your friendship and for your 20 years of exceptional service to the Department of Justi

[http://links.govdelivery.com:80/track?type=click&enid=ZWFzPTEmbWFpbGluZ2lkPTlwMTkwNDI2LjUxNzU2MTEmbWVzc2FnZWlkPU1EQi1QUkQtQlVMLTIwMTkwNDI2LjUxNzU2MTEmZGF0YWFhc2VpZD0xMDAxJnNlcmIhbD0xNzQ2NDM2MCZlbWVpbGlkPVJvYnluLkwuVGhpZW1hbm5AdXNkb2ouZ292JnVzZXJpZD1Sb2J5bi5MLIRoaWVtYW5uQHVzZG9qLmdvdiZmbD0mZXh0cmE9TXVsdGI2YXJpYXRISWQ9JiYm&&100&&https://www.justice.gov/?utm\\_medium=email&utm\\_source=govdelivery](http://links.govdelivery.com:80/track?type=click&enid=ZWFzPTEmbWFpbGluZ2lkPTlwMTkwNDI2LjUxNzU2MTEmbWVzc2FnZWlkPU1EQi1QUkQtQlVMLTIwMTkwNDI2LjUxNzU2MTEmZGF0YWFhc2VpZD0xMDAxJnNlcmIhbD0xNzQ2NDM2MCZlbWVpbGlkPVJvYnluLkwuVGhpZW1hbm5AdXNkb2ouZ292JnVzZXJpZD1Sb2J5bi5MLIRoaWVtYW5uQHVzZG9qLmdvdiZmbD0mZXh0cmE9TXVsdGI2YXJpYXRISWQ9JiYm&&100&&https://www.justice.gov/?utm_medium=email&utm_source=govdelivery)  
[REDACTED]

THURSDAY APRIL 27, 2019

# DEPUTY ATTORNEY GENERAL ROD J. ROSENSTEIN DELIVERS REMARKS AT THE ARMENIAN BAR ASSOCIATION'S PUBLIC SERVANTS DINNER

New York, New York

*Remarks as prepared for delivery*

"Peri yerego." Good evening.

Rick, I am grateful for your friendship and for your 20 years of exceptional service to the Department of Justice — including seven years as the United States Attorney for Northern New York.

I am pleased to see several U.S. Attorneys here tonight: Geoff Berman from Southern New York, Richard Donoghue from Eastern New York, Grant Jaquith from Northern New York, and Craig Carpenito from New Jersey; as well as eight former U.S. Attorneys, and many other current and former government employees.

I am thankful to Armenian Bar Association Chair Gerard Kassabian, and Vice Chairs Kathryn Ossian and Lucy Varpetian.

My wife served on your board of governors from 1993 to 2002. I got to know many of the members, particularly the group that traveled with us to Armenia in 1994 to celebrate the 75th anniversary of the University of Yerevan.

When I met Lisa in 1988, some of her relatives viewed me as "odan," an outsider to the culture. But recently a friend introduced me as "Armenian by Choice." After tonight, I have an even stronger claim to be an honorary Armenian.

"Shot Shenorhagal em." Thank you very much.

Our wedding featured an Armenian opera singer who is in the audience tonight, Maro Partamian. One of my favorite songs was "Lerner Hyreni," or "Mountains of Armenia." We hired the "Dark Eyes" band to play at the reception, which was great except that I chose a country song called "I Swear" by John Michael Montgomery for the first dance. It did not sound quite right with an Armenian accent.

One of Lisa's relatives was raised in Syria, where government service was not highly valued. Before he approved of the marriage, he wanted to know when I planned to get a real job, in the private sector.

Unfortunately, many native-born Americans also are skeptical about government service. My Uncle Harold was a self-employed carpet installer. One beautiful spring afternoon in 1994, I called him from an office in the Department of Justice headquarters building. It was a Saturday. And when I told him that I was working through the weekend, he said, "I'm sorry to hear that."

And I said, “You don’t understand. There is no place that I would rather be.”

I first walked into that building as a federal prosecutor on December 3, 1990, at age 25. I remember how honored I felt to represent the people of the United States. I will still feel the same way when I walk out for the last time next month.

I joined the Department of Justice because I believe in the mission. I stayed because I believe in the people who carry out the mission.

Our agents, analysts, and attorneys demonstrate great intellect and integrity. They possess superb academic credentials and exceptional character. They pass rigorous screening interviews and face thorough background checks every few years. They are ethical, honorable, and admirable people.

No organization with 115,000 employees is error-free. But we have serious, professional, nonpartisan internal watchdogs. We investigate credible misconduct allegations. We correct mistakes and punish wrongdoers.

I have served under five Presidents and nine Senate-confirmed Attorneys General — ten, if you count Bill Barr twice. I served mostly outside the D.C. beltway, but I worked at Department of Justice headquarters three times — four years in the early 1990s as a career prosecutor, four years in the early 2000s as a supervisor, and two years in my current job.

Our headquarters is a beautiful Depression-era building. I frequently speak about the inspiration that I draw from three aspects of the building – the art it contains; the people it employs; and the principles it represents.

There are reminders of heroes, mentors, and friends on every floor. They taught me that our Department stands for the principle that every American deserves the protection of the rule of law.

We use the term “rule of law” to describe our obligation to follow neutral principles. As President Trump pointed out, “we govern ourselves in accordance with the rule of law rather [than] ... the whims of an elite few or the dictates of collective will.”

Justice Anthony Kennedy explained it this way: in a rule of law system, when you apply to a government clerk for a permit and you satisfy the objective criteria, you are not asking for a favor. You are entitled to the permit, and it is the clerk’s duty to give it to you.

The idea that the government works for the people is relatively novel. In some countries, that concept of a government bound by law to serve the people does not exist.

When I visited Armenia in 1994, the nation was emerging from seven decades of Soviet domination. Gyumri and other northern cities were not yet rebuilt after the 1988 earthquake. The six-year war with Azerbaijan was halted by a recent ceasefire, but the blockade over Nagorno-Karabakh crippled the economy.

We flew on Air Armenia, which used a shabby old Russian jet. Our plane needed to stop for fuel in Bulgaria, and we heard that the pilots paid with cash.

Armenia faced many challenges in 1994. Many skilled and educated people had left the country. When we hired a taxi to visit Lake Sevan, the driver turned off the engine at every downhill stretch to conserve gasoline.

We stayed at a nice hotel near Republic Square, but some mornings there was no water to flush the toilets, and some evenings there was no electricity to cook the food.

I gave a lecture at the University of Yerevan about public corruption. When I finished, a student raised his hand. He asked, "If you can't pay bribes in America, then how do you get electricity?"

I repeat that question in many speeches. It usually elicits laughter. But the point is profound.

The question illustrates how that young man understood Soviet society. Corruption undermines law. It stifles innovation, creates inefficiency, and inculcates distrust.

The question explains why I devoted my career to law enforcement: because the rule of law is the foundation of human liberty. The rule of law secures our freedom. It will secure our children's freedom. And we can only achieve it if people who enforce the law set aside partisanship, because the rule of law requires a fair and independent process; a process where all citizens are equal in the eyes of the government.

I do not care how police officers, prosecutors, and judges vote, just as I do not care how soldiers and sailors vote. That is none of my business. I only care whether they understand that when they are on duty, their job is about law and not politics.

There is not Republican justice and Democrat justice. There is only justice and injustice.

In the courtyard of the Department of Justice headquarters, there is an inscription that reads, in Latin: "Privilegium Obligatio." It means that when you accept a privilege, you incur an obligation. Working for Justice is a privilege.

Our commensurate obligations are established by our oath to well and faithfully execute the duties of the office. To honor that oath, you need to know your office's unique duties. At our Department, our job is to seek the truth, apply the law, follow the Department's policies, and respect its principles.

The rule of law is our most important principle. Patriots must always defend the rule of law. Even when it is not in their personal interest, it is always in the national interest. If you find yourself asking, "What will this decision mean for me?" then you probably are not complying with your oath of office.

At my confirmation hearing in March 2017, a Republican Senator asked me to make a commitment. He said: "You're going to be in charge of this [Russia] investigation. I want you to look me in the eye and tell me that you'll do it right, that you'll take it to its conclusion and you'll report [your results] to the American people."

I did pledge to do it right and take it to the appropriate conclusion. I did not promise to report all results to the public, because grand jury investigations are ex parte proceedings. It is not our job to render conclusive factual findings. We just decide whether it is appropriate to file criminal charges.

Some critical decisions about the Russia investigation were made before I got there. The previous Administration chose not to publicize the full story about Russian computer hackers and social media trolls, and how they relate to a broader strategy to undermine America. The FBI disclosed classified



evidence about the investigation to ranking legislators and their staffers. Someone selectively leaked details to the news media. The FBI Director announced at a congressional hearing that there was a counterintelligence investigation that might result in criminal charges. Then the former FBI Director alleged that the President pressured him to close the investigation, and the President denied that the conversation occurred.

So that happened.

There is a story about firefighters who found a man on a burning bed. When they asked how the fire started, he replied, "I don't know. It was on fire when I lay down on it." I know the feeling.

But the bottom line is, there was overwhelming evidence that Russian operatives hacked American computers and defrauded American citizens, and that is only the tip of the iceberg of a comprehensive Russian strategy to influence elections, promote social discord, and undermine America, just like they do in many other countries.

In 1941, as Hitler sought to enslave Europe and Japan's emperor prepared to attack America, Attorney General Robert Jackson admonished federal prosecutors about their role in protecting national security. He said: "Defense is not only a matter of battleships and tanks, of guns and [soldiers].... It is raw materials, machines and [people who] work in factories. It is public morale. It is a law abiding population and a nation free from internal disorder . . . the ramparts we watch are not only those on the outer borders which are largely the concern of the military services. There are also the inner ramparts of our society — the Constitution, its guarantees, our freedoms and the supremacy of law. These are yours to guard and their protection is your defense program."

As acting Attorney General, it was my responsibility to make sure that the Department of Justice would do what the American people pay us to do: conduct an independent investigation; complete it expeditiously; hold perpetrators accountable if warranted; and work with partner agencies to counter foreign agents and deter crimes.

Today, our nation is safer, elections are more secure, and citizens are better informed about covert foreign influence schemes.

But not everybody was happy with my decision, in case you did not notice.

It is important to keep a sense of humor in Washington. You just need to accept that politicians need to evaluate everything in terms of the immediate political impact.

Then there are the mercenary critics, who get paid to express passionate opinions about any topic, often with little or no information. They do not just express disagreement. They launch ad hominem attacks unrestricted by truth or morality. They make threats, spread fake stories, and even attack your relatives. I saw one of the professional provocateurs at a holiday party. He said, "I'm sorry that I'm making your life miserable." And I said, "You do your job, and I'll do mine."

His job is to entertain and motivate partisans, so he can keep making money. My job is to enforce the law in a non-partisan way; that is the whole point of the oath of office.

In our Department, we disregard the mercenary critics and focus on the things that matter. As Goethe said, "Things that matter most must never be at the mercy of things that matter least." A republic that endures is not governed by the news cycle. Some of the nonsense that passes for breaking news

today would not be worth the paper was printed on, if anybody bothered to print it. It quickly fades away. The principles are what abide.

America's founders understood that the rule of law is not partisan. In 1770, five American colonists died after British soldiers fired on a crowd in the Boston Massacre. The soldiers were charged with murder. Many people believed that they deserved the death penalty.

John Adams agreed to represent the soldiers. His political beliefs were firmly against them. But Adams felt obligated to protect their rights under the law.

Defending British soldiers was a very unpopular cause, to put it mildly. Adams faced a serious risk, in his words, of "infamy," or even "death." In a diary entry about the trial, he wrote as follows: "In the evening I expressed to Mrs. Adams all my apprehensions: That excellent Lady, who has always encouraged me, burst into ... Tears.... [S]he was very sensible of all the danger to her and to our children as well as to me, but she thought I had done as I ought, [and] she was ... willing to share in all that was to come and place her trust in Providence."

The rhetoric mirrors an earlier letter that Adams wrote to explain his preference for integrity over acclaim. Adams wrote that in theaters "the applause of the audience is of more importance to the actors than their own approbation. But upon the stage of life, while conscience claps, let the world hiss."

Adams endured harsh criticism in the court of public opinion. But in the court of law, he secured the acquittal of the British captain and six soldiers.

At the trial, Adams delivered a timeless tribute to the rule of law. He said that "[f]acts are stubborn things; and whatever may be our wishes, our inclinations, or the dictates of our passions, they cannot alter the state of facts and evidence."

Adams' words remind us that people who seek the truth need to avoid confirmation bias. Truth is about solid evidence, not strong opinions. A 19th century Philadelphia doctor remarked that "sincerity of belief is not the test of truth." Many people passionately believe things that are not true.

I spent most of my career prosecuting cases in federal courthouses. My past trials in courts of law contrast with my recent tribulations in the halls of Congress, the channels of cable television, and the pages of the internet.

The difference is in the standard of proof. In my business, we need to prove facts with credible evidence, prove them beyond any reasonable doubt, and prove them to the unanimous satisfaction of a neutral judge and an unbiased jury of 12 random citizens.

Pursuing truth requires keeping an open mind, avoiding confirmation bias, and always yielding to credible evidence. Truth may not match our preconceptions. Truth may not satisfy our hopes. But truth is the foundation of the rule of law.

If lawyers cannot prove our case in court, then what we believe is irrelevant.

But in politics, belief is the whole ball game. In politics – as in journalism – the rules of evidence do not apply. That is not a critique. It is just an observation.

Last year, a congressman explained why he decided not to run for reelection. He said, “I like ... job[s] where facts matter. I like jobs where fairness matters. I like jobs where, frankly, ... the process matters.”

He was describing an American courtroom. “I like the art of persuasion,” he said. “I like finding 12 people who have not already made up their minds and ... may [let] the facts prevail. That’s not where we are in politics.”

That congressman spoke the truth. It may never be where we are in politics. But it must always be where we are in law.

Attorney General Jackson spoke about the fiduciary duty of government lawyers, the obligation to serve as a trustee for the public interest. He contrasted the special duties of government lawyers with what he called “the volatile values of politics.” That was in 1940.

Jackson understood that “lawyers must at times risk ourselves and our records to defend our legal processes from discredit, and to maintain a dispassionate, disinterested, and impartial enforcement of the law.”

“We must have the courage to face any temporary criticism,” Jackson urged, because “the moral authority of our legal process” depends on the commitment of government lawyers to act impartially.

Jackson also spoke about the role of lawyers in preserving liberty. He used a parable about three stonecutters asked to describe what they are doing. The first stonecutter focuses on how the job benefits him. He says, “I am earning a living.” The second narrowly describes his personal task: “I am cutting stone.” The third man has a very different perspective. His face lights up as he explains what the work means to others: “I am helping to build a cathedral.”

“[W]hether we are aware of it or not,” Jackson explained, lawyers “do more than earn [a] living[]; we do more than [litigate] [individual] cases. We are building the legal structure that will protect ... human liberty” for centuries to come.

As my time in public service comes to an end, I encourage each of you to remember the cathedral. You are always building a legacy. You set an example for your colleagues, and you lay a foundation for your successors.

Time flies when you get to work with good and honorable people. In the words of an Eagles song: “I’d do it all again; If I could somehow; But I must be leaving soon; It’s your world now... Use well your time; Be part of something good; Leave something good behind; ... It’s your world now.”

Ladies and gentlemen, this evening means a great deal to Lisa and me.

“Shot Shenorhagal-em yev Pari Keesher.” Thank you, and good night.

# # #



19-427

---

<http://links.gowdelivery.com:80/track?type=click&enid=ZWEEzPTEmbWEnpbGlluz22lkPTlwM>

---

[Department of Justice Privacy Policy](#) | [GovDelivery Privacy Policy](#)



THURSDAY APRIL 27, 2019

# **DEPUTY ATTORNEY GENERAL ROD J. ROSENSTEIN DELIVERS REMARKS AT THE ARMENIAN BAR ASSOCIATION'S PUBLIC SERVANTS DINNER**

**New York, New York**

***Remarks as prepared for delivery***

"Peri yerego." Good evening.

Rick, I am grateful for your friendship and for your 20 years of exceptional service to the Department of Justice — including seven years as the United States Attorney for Northern New York.

I am pleased to see several U.S. Attorneys here tonight: Geoff Berman from Southern New York, Richard Donoghue from Eastern New York, Grant Jaquith from Northern New York, and Craig Carpenito from New Jersey; as well as eight former U.S. Attorneys, and many other current and former government employees.

I am thankful to Armenian Bar Association Chair Gerard Kassabian, and Vice Chairs Kathryn Ossian and Lucy Varpetian.

My wife served on your board of governors from 1993 to 2002. I got to know many of the members, particularly the group that traveled with us to Armenia in 1994 to celebrate the 75th anniversary of the University of Yerevan.

When I met Lisa in 1988, some of her relatives viewed me as "odar," an outsider to the culture. But recently a friend introduced me as "Armenian by Choice." After tonight, I have an even stronger claim to be an honorary Armenian.

"Shot Shenorhagal em." Thank you very much.

Our wedding featured an Armenian opera singer who is in the audience tonight, Maro Partamian. One of my favorite songs was "Lerner Hyreni," or "Mountains of Armenia." We hired the "Dark Eyes" band to play at the reception, which was great except that I chose a country song called "I Swear" by John Michael Montgomery for the first dance. It did not sound quite right with an Armenian accent.

One of Lisa's relatives was raised in Syria, where government service was not highly valued. Before he approved of the marriage, he wanted to know when I planned to get a real job, in the private sector.



Unfortunately, many native-born Americans also are skeptical about government service. My Uncle Harold was a self-employed carpet installer. One beautiful spring afternoon in 1994, I called him from an office in the Department of Justice headquarters building. It was a Saturday. And when I told him that I was working through the weekend, he said, “I’m sorry to hear that.”

And I said, “You don’t understand. There is no place that I would rather be.”

I first walked into that building as a federal prosecutor on December 3, 1990, at age 25. I remember how honored I felt to represent the people of the United States. I will still feel the same way when I walk out for the last time next month.

I joined the Department of Justice because I believe in the mission. I stayed because I believe in the people who carry out the mission.

Our agents, analysts, and attorneys demonstrate great intellect and integrity. They possess superb academic credentials and exceptional character. They pass rigorous screening interviews and face thorough background checks every few years. They are ethical, honorable, and admirable people.

No organization with 115,000 employees is error-free. But we have serious, professional, nonpartisan internal watchdogs. We investigate credible misconduct allegations. We correct mistakes and punish wrongdoers.

I have served under five Presidents and nine Senate-confirmed Attorneys General — ten, if you count Bill Barr twice. I served mostly outside the D.C. beltway, but I worked at Department of Justice headquarters three times — four years in the early 1990s as a career prosecutor, four years in the early 2000s as a supervisor, and two years in my current job.

Our headquarters is a beautiful Depression-era building. I frequently speak about the inspiration that I draw from three aspects of the building – the art it contains; the people it employs; and the principles it represents.

There are reminders of heroes, mentors, and friends on every floor. They taught me that our Department stands for the principle that every American deserves the protection of the rule of law.

We use the term “rule of law” to describe our obligation to follow neutral principles. As President Trump pointed out, “we govern ourselves in accordance with the rule of law rather [than] ... the whims of an elite few or the dictates of collective will.”

Justice Anthony Kennedy explained it this way: in a rule of law system, when you apply to a government clerk for a permit and you satisfy the objective criteria, you are not asking for a favor. You are entitled to the permit, and it is the clerk’s duty to give it to you.

The idea that the government works for the people is relatively novel. In some countries, that concept of a government bound by law to serve the people does not exist.

When I visited Armenia in 1994, the nation was emerging from seven decades of Soviet domination. Gyumri and other northern cities were not yet rebuilt after the 1988 earthquake. The six-year war with Azerbaijan was halted by a recent ceasefire, but the blockade over Nagorno-Karabakh crippled the economy.

We flew on Air Armenia, which used a shabby old Russian jet. Our plane needed to stop for fuel in Bulgaria, and we heard that the pilots paid with cash.

Armenia faced many challenges in 1994. Many skilled and educated people had left the country. When we hired a taxi to visit Lake Sevan, the driver turned off the engine at every downhill stretch to conserve gasoline.

We stayed at a nice hotel near Republic Square, but some mornings there was no water to flush the toilets, and some evenings there was no electricity to cook the food.

I gave a lecture at the University of Yerevan about public corruption. When I finished, a student raised his hand. He asked, "If you can't pay bribes in America, then how do you get electricity?"

I repeat that question in many speeches. It usually elicits laughter. But the point is profound.

The question illustrates how that young man understood Soviet society. Corruption undermines law. It stifles innovation, creates inefficiency, and inculcates distrust.

The question explains why I devoted my career to law enforcement: because the rule of law is the foundation of human liberty. The rule of law secures our freedom. It will secure our children's freedom. And we can only achieve it if people who enforce the law set aside partisanship, because the rule of law requires a fair and independent process; a process where all citizens are equal in the eyes of the government.

I do not care how police officers, prosecutors, and judges vote, just as I do not care how soldiers and sailors vote. That is none of my business. I only care whether they understand that when they are on duty, their job is about law and not politics.

There is not Republican justice and Democrat justice. There is only justice and injustice.

In the courtyard of the Department of Justice headquarters, there is an inscription that reads, in Latin: "Privilegium Obligatio." It means that when you accept a privilege, you incur an obligation. Working for Justice is a privilege.

Our commensurate obligations are established by our oath to well and faithfully execute the duties of the office. To honor that oath, you need to know your office's unique duties. At our Department, our job is to seek the truth, apply the law, follow the Department's policies, and respect its principles.

The rule of law is our most important principle. Patriots must always defend the rule of law. Even when it is not in their personal interest, it is always in the national interest. If you find yourself asking, "What will this decision mean for me?" then you probably are not complying with your oath of office.

At my confirmation hearing in March 2017, a Republican Senator asked me to make a commitment. He said: "You're going to be in charge of this [Russia] investigation. I want you to look me in the eye and tell me that you'll do it right, that you'll take it to its conclusion and you'll report [your results] to the American people."

I did pledge to do it right and take it to the appropriate conclusion. I did not promise to report all results to the public, because grand jury investigations are ex parte proceedings. It is not our job to render conclusive factual findings. We just decide whether it is appropriate to file criminal charges.

Some critical decisions about the Russia investigation were made before I got there. The previous Administration chose not to publicize the full story about Russian computer hackers and social media trolls, and how they relate to a broader strategy to undermine America. The FBI disclosed classified evidence about the investigation to ranking legislators and their staffers. Someone selectively leaked details to the news media. The FBI Director announced at a congressional hearing that there was a counterintelligence investigation that might result in criminal charges. Then the former FBI Director alleged that the President pressured him to close the investigation, and the President denied that the conversation occurred.

So that happened.

There is a story about firefighters who found a man on a burning bed. When they asked how the fire started, he replied, "I don't know. It was on fire when I lay down on it." I know the feeling.

But the bottom line is, there was overwhelming evidence that Russian operatives hacked American computers and defrauded American citizens, and that is only the tip of the iceberg of a comprehensive Russian strategy to influence elections, promote social discord, and undermine America, just like they do in many other countries.

In 1941, as Hitler sought to enslave Europe and Japan's emperor prepared to attack America, Attorney General Robert Jackson admonished federal prosecutors about their role in protecting national security. He said: "Defense is not only a matter of battleships and tanks, of guns and [soldiers].... It is raw materials, machines and [people who] work in factories. It is public morale. It is a law abiding population and a nation free from internal disorder . . . the ramparts we watch are not only those on the outer borders which are largely the concern of the military services. There are also the inner ramparts of our society — the Constitution, its guarantees, our freedoms and the supremacy of law. These are yours to guard and their protection is your defense program."

As acting Attorney General, it was my responsibility to make sure that the Department of Justice would do what the American people pay us to do: conduct an independent investigation; complete it expeditiously; hold perpetrators accountable if warranted; and work with partner agencies to counter foreign agents and deter crimes.

Today, our nation is safer, elections are more secure, and citizens are better informed about covert foreign influence schemes.

But not everybody was happy with my decision, in case you did not notice.

It is important to keep a sense of humor in Washington. You just need to accept that politicians need to evaluate everything in terms of the immediate political impact.

Then there are the mercenary critics, who get paid to express passionate opinions about any topic, often with little or no information. They do not just express disagreement. They launch ad hominem attacks unrestricted by truth or morality. They make threats, spread fake stories, and even attack your relatives. I saw one of the professional provocateurs at a holiday party. He said, "I'm sorry that I'm making your life miserable." And I said, "You do your job, and I'll do mine."

His job is to entertain and motivate partisans, so he can keep making money. My job is to enforce the law in a non-partisan way; that is the whole point of the oath of office.

In our Department, we disregard the mercenary critics and focus on the things that matter. As Goethe said, “Things that matter most must never be at the mercy of things that matter least.” A republic that endures is not governed by the news cycle. Some of the nonsense that passes for breaking news today would not be worth the paper was printed on, if anybody bothered to print it. It quickly fades away. The principles are what abide.

America’s founders understood that the rule of law is not partisan. In 1770, five American colonists died after British soldiers fired on a crowd in the Boston Massacre. The soldiers were charged with murder. Many people believed that they deserved the death penalty.

John Adams agreed to represent the soldiers. His political beliefs were firmly against them. But Adams felt obligated to protect their rights under the law.

Defending British soldiers was a very unpopular cause, to put it mildly. Adams faced a serious risk, in his words, of “infamy,” or even “death.” In a diary entry about the trial, he wrote as follows: “In the evening I expressed to Mrs. Adams all my apprehensions: That excellent Lady, who has always encouraged me, burst into ... Tears.... [S]he was very sensible of all the danger to her and to our children as well as to me, but she thought I had done as I ought, [and] she was ... willing to share in all that was to come and place her trust in Providence.”

The rhetoric mirrors an earlier letter that Adams wrote to explain his preference for integrity over acclaim. Adams wrote that in theaters “the applause of the audience is of more importance to the actors than their own approbation. But upon the stage of life, while conscience claps, let the world hiss.”

Adams endured harsh criticism in the court of public opinion. But in the court of law, he secured the acquittal of the British captain and six soldiers.

At the trial, Adams delivered a timeless tribute to the rule of law. He said that “[f]acts are stubborn things; and whatever may be our wishes, our inclinations, or the dictates of our passions, they cannot alter the state of facts and evidence.”

Adams’ words remind us that people who seek the truth need to avoid confirmation bias. Truth is about solid evidence, not strong opinions. A 19th century Philadelphia doctor remarked that “sincerity of belief is not the test of truth.” Many people passionately believe things that are not true.

I spent most of my career prosecuting cases in federal courthouses. My past trials in courts of law contrast with my recent tribulations in the halls of Congress, the channels of cable television, and the pages of the internet.

The difference is in the standard of proof. In my business, we need to prove facts with credible evidence, prove them beyond any reasonable doubt, and prove them to the unanimous satisfaction of a neutral judge and an unbiased jury of 12 random citizens.

Pursuing truth requires keeping an open mind, avoiding confirmation bias, and always yielding to credible evidence. Truth may not match our preconceptions. Truth may not satisfy our hopes. But truth is the foundation of the rule of law.

If lawyers cannot prove our case in court, then what we believe is irrelevant.

But in politics, belief is the whole ball game. In politics – as in journalism – the rules of evidence do not apply. That is not a critique. It is just an observation.

Last year, a congressman explained why he decided not to run for reelection. He said, “I like ... job[s] where facts matter. I like jobs where fairness matters. I like jobs where, frankly, ... the process matters.”

He was describing an American courtroom. “I like the art of persuasion,” he said. “I like finding 12 people who have not already made up their minds and ... may [let] the facts prevail. That’s not where we are in politics.”

That congressman spoke the truth. It may never be where we are in politics. But it must always be where we are in law.

Attorney General Jackson spoke about the fiduciary duty of government lawyers, the obligation to serve as a trustee for the public interest. He contrasted the special duties of government lawyers with what he called “the volatile values of politics.” That was in 1940.

Jackson understood that “lawyers must at times risk ourselves and our records to defend our legal processes from discredit, and to maintain a dispassionate, disinterested, and impartial enforcement of the law.”

“We must have the courage to face any temporary criticism,” Jackson urged, because “the moral authority of our legal process” depends on the commitment of government lawyers to act impartially.

Jackson also spoke about the role of lawyers in preserving liberty. He used a parable about three stonecutters asked to describe what they are doing. The first stonecutter focuses on how the job benefits him. He says, “I am earning a living.” The second narrowly describes his personal task: “I am cutting stone.” The third man has a very different perspective. His face lights up as he explains what the work means to others: “I am helping to build a cathedral.”

“[W]hether we are aware of it or not,” Jackson explained, lawyers “do more than earn [a] living[]; we do more than [litigate] [individual] cases. We are building the legal structure that will protect ... human liberty” for centuries to come.

As my time in public service comes to an end, I encourage each of you to remember the cathedral. You are always building a legacy. You set an example for your colleagues, and you lay a foundation for your successors.

Time flies when you get to work with good and honorable people. In the words of an Eagles song: “I’d do it all again; If I could somehow; But I must be leaving soon; It’s your world now... Use well your time; Be part of something good; Leave something good behind; ... It’s your world now.”

Ladies and gentlemen, this evening means a great deal to Lisa and me.

“Shot Shenorhagal-em yev Pari Keesher.” Thank you, and good night.

# # #



[illegible]

[Department of Justice Privacy Policy](#) | [GovDelivery Privacy Policy](#)

8



---

**From:** Sutton, Sarah E. (OPA)  
**Sent:** Friday, April 26, 2019 1:53 PM  
**To:** Rosenstein, Rod (ODAG)  
**Subject:** DAG Rosenstein Speaks at the Armenian Bar Association Media Report.docx  
**Attachments:** DAG Rosenstein Speaks at the Armenian Bar Association Media Report.docx;  
ATT00001.txt

Working on NYT piece, but want to send these along in the meantime.

# DAG Rosenstein Speaks at the Armenian Bar Association's Public Servants Dinner—Media Report

*As of: April 26, 2019,*

## **Video Clips:**

[Rosenstein defends his role in Mueller investigation](#) CNN

[Rod Rosenstein criticizes the Obama administration for their handling of the Russia investigation](#)

## **Print (Headlines, Full Text Below):**

[Rosenstein fires back at critics over Mueller report](#) Washington Post

[Rosenstein defends Russia investigation, takes shots at Obama administration](#) Politico

[Rod Rosenstein shares his thinking about the Mueller investigation](#) CBS News

[Rosenstein unloads on critics, defends handling of Russia investigation](#) CNN

[Rosenstein hits at Obama for hiding that Russian trolls were infiltrating 2016 election](#)  
Washington Examiner

[Rosenstein speaks out to defend Russia probe, rip Obama administration](#) NBC News

[Rosenstein Takes Aim at Critics, Defends Role in Mueller Investigation](#) Wall Street Journal

[Rosenstein slams Obama administration for choosing ‘not to publicize full story’ of Russia hacking](#) Fox News

[Deputy AG Rod Rosenstein offers staunch defense of Russia investigation, jabs Obama administration](#) USA Today

[Rosenstein Lashes Out at Obama and the Media, Defends Trump in First Remarks Since Mueller Report](#) Daily Beast

[Rod Rosenstein Defends Handling Of Mueller Report](#) Daily Caller

## **Full Text:**

[Rosenstein fires back at critics over Mueller report](#) Washington Post

NEW YORK — Deputy Attorney General Rod J. Rosenstein hit back hard against politicians and the press Thursday night, and warned that hacking and social media manipulation are “only the tip of the iceberg” when it comes to Russian efforts to influence American elections.

Speaking at the Public Servants Dinner of the Armenian Bar Association, Rosenstein unleashed his sharpest critique yet of those who have attacked his handling of special counsel Robert S. Mueller III's investigative report into Russian election interference and President Trump's conduct.

Rosenstein's speech, probably one of his last as a senior Justice Department official, marked his first public comments since the release of the report, and he did not hold back in discussing his tumultuous two years as the No. 2 at the Justice Department. During that time, he was castigated by both Republicans and Democrats for a variety of decisions. In the speech, Rosenstein reflected on his time on the job, spoke positively of Trump's commitment to the rule of law and criticized the press.

He also said that, even after the Mueller report documented Russian interference in the 2016 election, that is only a small part of the story.

"The bottom line is, there was overwhelming evidence that Russian operatives hacked American computers and defrauded American citizens, and that is only the tip of the iceberg of a comprehensive Russian strategy to influence elections, promote social discord, and undermine America, just like they do in many other countries," Rosenstein said.

Rosenstein appointed Mueller as special counsel in May 2017, and has overseen the investigation since. Now that Mueller's work is over and Trump has nominated someone else to be the No. 2 official at the Justice Department, Rosenstein is expected to leave the job as early as next month.

In his speech, Rosenstein critiqued Congress, politics and the media, and defended the Justice Department as an institution whose mission is to rise above partisanship and focus on facts.

"I do not care how police officers, prosecutors and judges vote, just as I do not care how soldiers and sailors vote. That is none of my business. I only care whether they understand that when they are on duty, their job is about law and not politics," said Rosenstein, who has worked at the Justice Department for decades.

"There is not Republican justice and Democrat justice. There is only justice and injustice," he said.

In his speeches, Rosenstein often refers positively to Trump, and he did so again on Thursday, a week after the Justice Department issued nearly 200 pages of findings documenting instances in which prosecutors and federal agents were concerned the president might have obstructed justice.

Ultimately, Mueller did not make a determination as to whether the president broke the law, based partly on the Justice Department's long-standing policy that a sitting president cannot be charged with a crime while in office. Attorney General William P. Barr reviewed Mueller's findings last month and declared that both he and Rosenstein had determined the president had not obstructed justice.

"The rule of law is our most important principle," Rosenstein said. "As President Trump pointed out, 'We govern ourselves in accordance with the rule of law rather [than] ... the whims of an elite few or the dictates of collective will.' "

The deputy attorney general recalled that at his confirmation hearing, he made promises about how the Russia investigation would be handled.

"I did pledge to do it right and take it to the appropriate conclusion. I did not promise to report all results to the public, because grand jury investigations are ex parte proceedings. It is not our job to render conclusive factual findings," he said. "We just decide whether it is appropriate to file criminal charges."

Leading up to the release of the Mueller report, Rosenstein had argued against too much transparency, citing Justice Department policies that generally don't reveal derogatory information about people who have not been charged with a crime, according to people familiar with the discussions. Ultimately, Barr decided to publicly release more.

Rosenstein insisted the investigation had been conducted fairly and conscientiously, and that as a result, "our nation is safer, elections are more secure, and citizens are better informed about covert foreign influence schemes. But not everybody was happy with my decision, in case you did not notice."

He denounced what he called “mercenary critics, who get paid to express passionate opinions about any topic, often with little or no information. They do not just express disagreement. They launch ad hominem attacks unrestricted by truth or morality. They make threats, spread fake stories and even attack your relatives.”

Rosenstein also took some shots at the press.

“Some of the nonsense that passes for breaking news today would not be worth the paper it was printed on, if anybody bothered to print it,” he said. “One silly question that I get from reporters is, ‘Is it true that you got angry and emotional a few times over the past few years?’ Heck yes! Didn’t you?”

He also tried to joke off questions that emerged over his appearance last week at Barr’s press conference ahead of the release of the Mueller report, in which he appeared ashen-faced.

“Last week, the big topic of discussion was: ‘What were you thinking when you stood behind Bill Barr at that press conference, with a deadpan expression?’ The answer is: I was thinking, ‘My job is to stand here with a deadpan expression.’ ”

The audience applauded.

“Can you imagine if I did anything other than stand there at the press conference? Imagine the reaction and the commentary if I had smiled or grimaced,” Rosenstein said. “But you cannot avoid criticism. The only way you can avoid criticism in public service is if you stay home. But somebody actually has to do the work, and therefore you have to accept the criticism that comes with the job.”

The evening’s other honoree was Robert Tembeckjian, administrator of New York State’s Commission on Judicial Conduct. Rosenstein chatted with the others at his table and checked his phone as Tembeckjian unleashed a steady stream of criticism against the administration’s immigration policies. The crowd applauded as Tembeckjian warned of the path to tyranny and celebrated his own family’s history as undocumented immigrants from Armenia.

Tembeckjian also earned some laughs at the president's expense, after mentioning Rosenstein's pending departure from government.

"I can tell by the absence of Secret Service," he said, "that the person most eager to see him leave is not here tonight."

#### [Rosenstein defends Russia investigation, takes shots at Obama administration](#) Politico

Deputy Attorney General Rod Rosenstein on Thursday teed off on the Obama administration's handling of Russian election interference and hit back at critics of the Russia probe in his first public remarks since special counsel Robert Mueller's report dropped last week.

Speaking at the Public Servants Dinner of the Armenian Bar Association, Rosenstein said he and other top Justice Department officials went above and beyond their responsibilities when it came to the investigation.

Rosenstein cited a line of questioning he faced at his confirmation hearing in 2017, before he officially took on the investigation, pointing out that he made no promises once it had concluded "to report all results to the public, because grand jury investigations are ex parte proceedings."

He also defended the outcome of the probe, pointing to how it "does not conclude that the President committed a crime, it also does not exonerate him."

"It is not our job to render conclusive factual findings. We just decide whether it is appropriate to file criminal charges," Rosenstein said, in what also could have been taken as a swipe at those who have insisted Mueller was wrong not to bring charges against the president. Trump's defenders have criticized Mueller for trying to "prove a negative" on obstruction of justice.

He then chastised "critical decisions" he said had been made about the investigation before he arrived by the Obama administration and then-FBI director James Comey, including not divulging more about Russia's meddling. He compared the atmosphere of his time as DOJ's No. 2 to a parable about a man who laid down on a burning bed.

"The previous administration chose not to publicize the full story about Russian computer hackers and social media trolls, and how they relate to a broader strategy to undermine



America,” he said. “The FBI disclosed classified evidence about the investigation to ranking legislators and their staffers. Someone selectively leaked details to the news media. The FBI director announced at a congressional hearing that there was a counterintelligence investigation that might result in criminal charges. Then the former FBI director alleged that the President pressured him to close the investigation, and the President denied that the conversation occurred. So that happened.”

Still, he defended the investigation and its findings in his speech, as well as DOJ’s dedication to the rule of law and staying above the fray of partisanship, declaring that “today, our nation is safer, elections are more secure, and citizens are better informed about covert foreign influence schemes.”

But, he acknowledged, “not everybody was happy with my decision, in case you did not notice.”

Rosenstein blasted “mercenary critics” who “express passionate opinions about any topic, often with little or no information” and “launch ad hominem attacks unrestricted by truth or morality,” as well as the press and Congress.

“Some of the nonsense that passes for breaking news today would not be worth the paper it was printed on, if anybody bothered to print it,” he said, noting that his recent experiences dealing with Congress and the media were starkly different than the court environment he was accustomed to.

“The difference is in the standard of proof. In my business, we need to prove facts with credible evidence, prove them beyond any reasonable doubt, and prove them to the unanimous satisfaction of a neutral judge and an unbiased jury of 12 random citizens,” Rosenstein said, comparing it to politics and the journalism where he asserted “belief is the whole ball game.”

[Rod Rosenstein shares his thinking about the Mueller investigation](#) CBS News

Deputy Attorney General Rod Rosenstein shared some of his thoughts about his approach to and origins of the special counsel's investigation. At a speech at an Armenian Bar Association dinner Thursday, Rosenstein recalled that two years ago, at his confirmation hearing, a GOP senator told him he'd be charged with the Russia probe and demanded that Rosenstein promise to "do it right."

"You're going to be in charge of this [Russia] investigation. I want you to look me in the eye and tell me that you'll do it right, that you'll take it to its conclusion and you'll report [your results] to the American people," he said the senator told him.

Rosenstein agreed to the first two things the senator asked, but then explained, "I did not promise to report all results to the public, because grand jury investigations are ex parte proceedings. It is not our job to render conclusive factual findings. We just decide whether it is appropriate to file criminal charges."

He said that there were "some critical decisions" about the investigation that had been made before he was on the job as deputy attorney general. The Obama administration, he said, "chose not to publicize the full story about Russian computer hackers and social media trolls, and how they relate to a broader strategy to undermine America."

And the FBI had given classified evidence about the investigation to top lawmakers and their staff, and "someone selectively leaked details to the news media."

He then reminded his audience that then-FBI Director James Comey disclosed during a congressional hearing that "there was a counterintelligence investigation that might result in criminal charges."

"Then the former FBI Director alleged that the president pressured him to close the investigation, and the president denied that the conversation occurred," he continued.

"So that happened," he deadpanned.

Because then-Attorney General Jeff Sessions had recused himself from the Russia investigation, it fell to Rosenstein to oversee it after President Trump fired Comey.

"As acting Attorney General, it was my responsibility to make sure that the Department of Justice would do what the American people pay us to do: conduct an independent investigation," Rosenstein said, and "complete it expeditiously."

At the end of the special counsel's investigation, Rosenstein said, "[O]ur nation is safer, elections are more secure, and citizens are better informed about covert foreign influence schemes." But he noted that "not everybody was happy with my decision, in case you did not notice."

However, Rosenstein, who leaves the Justice Department next month, seemed to shrug off the months of invective leveled at him over the investigation. He's taking a longer view, it appears. Rosenstein quoted former Attorney General Robert Jackson, who said about 80 years ago, "'We must have the courage to face any 'temporary criticism' because 'the moral authority of our legal process' depends on the commitment of government lawyers to act impartially.'"

[Rosenstein unloads on critics, defends handling of Russia investigation](#) CNN

Deputy Attorney General Rod Rosenstein defended his handling of the Russia investigation Thursday evening, recalling how he had promised to "do it right" during his Senate confirmation hearing and "take it to the appropriate conclusion," while taking pointed swipes at what he called "mercenary critics," politicians and the news media.

"It's not our job to render conclusive factual findings. We just decide whether it is appropriate to file criminal charges," Rosenstein said, speaking at a dinner in New York where he was honored by the Armenian Bar Association.

The redacted report released last week concluding special counsel Robert Mueller's investigation indicated that prosecutors ultimately did not make a decision on whether President Donald Trump had obstructed justice. But prosecutors did not exonerate him of criminal conduct, and determined that Congress still has the ability to find he obstructed justice.

Rosenstein went on to argue Thursday night that "some critical decisions" had been made before his tenure as the deputy attorney general. The previous administration "chose not to publicize the full story about Russian computer hackers and social media trolls" but the story later leaked to the media, he argued, and then-FBI Director James Comey then told Congress there was a counterintelligence investigation and alleged that Trump "pressured him to close the investigation."

"So that happened," Rosenstein said to laughter from the audience, before highlighting Mueller's findings of extensive Russian interference in the 2016 presidential election.

"The bottom line is that there was overwhelming evidence that Russian operatives had hacked American computers and defrauded American citizens, and that was only the tip of the iceberg of a comprehensive Russian strategy to influence elections, promote social discord and undermine America," he added.

Rosenstein stood by his decision to appoint Mueller, despite the fact that "not everybody was happy with my decision, in case you didn't notice" -- a possible reference to Trump's vocal and long-standing misgivings about the need for and motivations of the special counsel's team.

"You just need to accept that politicians need to evaluate everything in terms of the immediate political impact," Rosenstein added.

He also addressed reports of his emotions getting the better of him at stressful moments during the investigation, saying that one "silly question that I get from reporters" is whether it's true that he ever got angry.

"Heck, yes, didn't you?" he said.

Finally he addressed his "deadpan" facial expressions at Attorney General William Barr's news conference last week just prior to the report's release.

"The answer is, I was thinking, 'My job is to stand here with a deadpan expression,' " Rosenstein joked, adding, "Can you imagine if I did anything other than a deadpan reaction?"

Rosenstein also mentioned that he would be leaving the Department of Justice "next month." He was originally expected to leave earlier this year, but the departure date has been something of a moving target, as CNN has previously reported. Jeffrey Rosen, the deputy transportation secretary, who Trump nominated to replace Rosenstein, is still awaiting a vote on his confirmation in the Senate.

[Rosenstein hits at Obama for hiding that Russian trolls were infiltrating 2016 election](#)

Washington Examiner

Deputy Attorney General Rod Rosenstein, who appointed special counsel Robert Mueller to investigate Russian election meddling, had a few things to say about the way it started.

Starting with the Obama administration.

"The previous Administration chose not to publicize the full story about Russian computer hackers and social media trolls, and how they relate to a broader strategy to undermine America," he said.

Rosenstein punched back at critics during a speech at the Armenian Bar Association's Public Servants Dinner in New York City on Thursday, where he defended the Department of Justice's handling of the investigation and his role in it.

"There was overwhelming evidence that Russian operatives hacked American computers and defrauded American citizens, and that is only the tip of the iceberg of a comprehensive Russian strategy to influence elections, promote social discord, and undermine America, just like they do in many other countries," he said.

But it wasn't for the DOJ to make an ultimate finding.

"I did pledge to do it right and take it to the appropriate conclusion. I did not promise to report all results to the public, because grand jury investigations are ex parte proceedings. It is not our job to render conclusive factual findings. We just decide whether it is appropriate to file criminal charges," he said.

The Justice Department came under fire from critics following the release of the 448-page Mueller report. A four-page summary by Attorney General William Barr that determined that while Russia had interfered in the 2016 presidential election, the Trump campaign did not collude with the effort.

While Mueller said did not draw a conclusion about whether President Trump obstructed justice, saying the report "also does not exonerate him," Barr and Rosenstein concluded there was not sufficient evidence to determine whether Trump did so.

[Rosenstein speaks out to defend Russia probe, rip Obama administration](#) NBC News

Rod Rosenstein, the deputy attorney general who supervised special counsel Robert Mueller's investigation into Russian election interference and President Donald Trump, on Thursday defended his handling of the probe, trashed the media for the way it was covered and slammed the Obama administration for not revealing "the full story" about Russia's efforts.

"Some critical decisions about that Russia investigation were made before I got there. The previous administration chose not to publicize the full story about Russian computer hackers and social media trolls, and how they relate to Russia's broader strategy to undermine America," Rosenstein told the Armenian Bar Association's Public Servants Dinner in New York.

The speech marked the first time Rosenstein has spoken publicly since Attorney General William Barr, earlier this month, released a redacted copy of Mueller's report detailing his findings. While finding no criminal conspiracy, the report showed that Trump associates met with Russians after the intelligence community said in October 2016 that Russia was interfering in the presidential election, and even after the Obama administration announced a set of post-election sanctions to punish Russia for that behavior. Mueller's report also details 10 episodes of potential obstruction by Trump, but did not conclude whether the president committed a crime. The report "also does not exonerate him," Mueller wrote. Barr declared, in a letter to Congress prior to the redacted report's release, that Trump did not obstruct justice.

Rosenstein on Thursday also criticized former FBI Director James Comey for an array of decisions he'd made about the agency's probe into Russian interference.

"The FBI disclosed classified evidence about the investigation to ranking legislators and their staffers. Someone selectively leaked details to the news media. The FBI director announced at a congressional hearing that there was a counterintelligence investigation that might result in criminal charges. Then the former FBI director alleged that the president pressured him to close the investigation, and the president denied that the conversation occurred," Rosenstein said.

Mueller's report lays out evidence that appears to support Comey's version of the events leading up to his firing, which the White House initially pinned on a memo drafted by Rosenstein at Trump's request. Rosenstein's memo attributed the rationale for dismissing the FBI chief to Comey's handling of the probe into Hillary Clinton's use of a private email server while secretary of state.

According to Mueller's report, however, "substantial evidence indicates that the catalyst for the president's decision to fire Comey was Comey's unwillingness to publicly state that the



president was not personally under investigation, despite the president's repeated requests that Comey make such an announcement."

Later in the speech, Rosenstein took a swipe at the media for how it covered the investigation, hitting "mercenary critics" who "get paid to express passionate opinions about any topic, often with little or no information" and who "launch ad hominem attacks unrestricted by truth or morality."

"Some of the nonsense that passes for breaking news today would not be worth the paper was printed on, if anybody bothered to print it," he said. "It quickly fades away. The principles are what abide."

Above all, Rosenstein defended how the investigation was handled, saying he had promised to "do it right."

"I did pledge to do it right and take it to the appropriate conclusion. I did not promise to report all results to the public, because grand jury investigations are ex parte proceedings. It is not our job to render conclusive factual findings. We just decide whether it is appropriate to file criminal charges," Rosenstein said.

[Rosenstein Takes Aim at Critics, Defends Role in Mueller Investigation](#) Wall Street Journal

The U.S. is safer and better informed about Russian election interference because of special counsel Robert Mueller's investigation, Deputy Attorney General Rod Rosenstein said Thursday night in a fiery speech in which he lashed out at critics and defended the decisions that defined his time in office.

In his first public remarks since the release of Mr. Mueller's report, Mr. Rosenstein criticized the Obama administration as being slow to publicly address Russia's efforts to undermine U.S. elections and slammed former FBI Director James Comey for announcing to Congress that the agency was investigating whether the Trump campaign colluded with Moscow.

"Then the former FBI director alleged that the president pressured him to close the investigation, and the President denied that the conversation occurred," Mr. Rosenstein said, reflecting on the events that led him to appoint the special counsel in May 2017. "So that happened."

The deputy attorney general, in his waning days on the job, was speaking to the Armenian Bar Association, where his wife was once a board member. He recalled visits to the country in the early 1990s as it was emerging from Soviet control.

He went on to defend his role in Mr. Mueller's investigation, which found President Trump and his campaign didn't conspire with Russia to interfere in the 2016 presidential election but didn't conclude whether or not Mr. Trump obstructed justice. Still, the 448-page report that Attorney General William Barr released last week outlined the president's efforts to shut down or curtail the investigation. In the absence of a recommendation from Mr. Mueller's team, Mr. Barr, working with Mr. Rosenstein, determined that conduct didn't amount to a crime.

Mr. Rosenstein recalled promises he made during his confirmation hearing to properly handle the probe.

"I did not promise to report all results to the public, because grand jury investigations are ex parte proceedings," he said. "It is not our job to render conclusive factual findings. We just decide whether it is appropriate to file criminal charges."

Mr. Rosenstein didn't say what he thought of Mr. Barr's handling of the report but joked about speculation over his physical appearance during a news conference ahead of the report's release, where he stood behind the attorney general, stone-faced and silent.

"Last week, the big topic of discussion was, what were you thinking when you stood behind Bill Barr at that press conference, with a deadpan expression? The answer is, I was thinking, 'My job is to stand here with a deadpan expression'."

Mr. Rosenstein, 54, will soon leave the Justice Department after nearly 30 years there, but hasn't said what he will do next. He was under an unusually intense spotlight as deputy attorney general, largely because of his decision to appoint Mr. Mueller early in his tenure, which enraged Mr. Trump. He had assumed oversight of the investigation from then-Attorney General Jeff Sessions, who had recused himself, citing his own role in Mr. Trump's campaign. In a separate speech Wednesday, Mr. Sessions said it was time to accept the results of Mr. Mueller's investigation and "get on with the business of America."

Mr. Rosenstein said he appointed the special counsel because he had a responsibility to make sure the Justice Department conducted an independent investigation, completed it quickly and brought criminal charges where warranted.

“But not everybody was happy with my decision, in case you did not notice,” he said. “It is important to keep a sense of humor in Washington. You just need to accept that politicians need to evaluate everything in terms of the immediate political impact.”

The bottom line, Mr. Rosenstein said, is that the kind of computer hacking and social-media manipulation the investigation revealed are “only the tip of the iceberg of a comprehensive Russian strategy to influence elections, promote social discord, and undermine America, just like they do in many other countries.”

Turning his attention to the news media, Mr. Rosenstein said: “Some of the nonsense that passes for breaking news today would not be worth the paper it was printed on, if anybody bothered to print it,” he said. “One silly question that I get from reporters is, ‘Is it true that you got angry and emotional a few times over the past few years?’ Heck yes! Didn’t you?”

He also fired back at what he called “mercenary critics” who “make threats, spread fake stories, and even attack your relatives ... I saw one of the professional provocateurs at a holiday party. He said, ‘I’m sorry that I’m making your life miserable.’ And I said, ‘You do your job, and I’ll do mine.’”

[Rosenstein slams Obama administration for choosing ‘not to publicize full story’ of Russia hacking](#) Fox News

Beleaguered Justice Department No. 2 Rod Rosenstein raised eyebrows Thursday night with a private speech in which he took a swipe at the Obama administration and slammed ex-FBI boss James Comey.

Rosenstein, the U.S. deputy attorney general who supervised the Mueller investigation, spoke out publicly for the first time since the report was released, criticizing the Obama administration’s real-time reaction to Russian hacking and its decision “not to publicize the full story” to the American people.

Rosenstein, who was speaking in New York at the Public Servants Dinner of the Armenian Bar Association, defended his handling of the probe and criticized former officials in the process. He also called out former FBI Director James Comey for alerting Congress about the investigation into Russian collusion at the height of the 2016 presidential campaign.

“The FBI disclosed classified evidence about the investigation to ranking legislators and their staffers,” he said. “Someone selectively leaked details to the news media. The FBI director [Comey] announced at a congressional hearing that there was a counterintelligence investigation that might result in criminal charges. Then the former FBI director alleged that the president pressured him to close the investigation, and the president denied that the conversation occurred.

"So that happened," he joked.

The Obama administration has been criticized for its handling of the Russian interference. Trump has blamed Obama for not acting quickly enough to stem Russia's influence during the campaign.

In 2016, NBC News, citing unnamed high-level officials, reported that the Obama administration did not respond more forcefully because it did not want to appear to be interfering with the election. One official told the network at the time, "They thought [Hillary Clinton] was going to win, so they were willing to kick the can down the road."

A reporter for NPR said the Obama administration debated how to handle the information and decided that Obama should deal with Russian President Vladimir Putin privately about the matter.

The Rosenstein speech touched on a lot of topics.

He blasted “mercenary critics” who benefit financially by expressing “passionate opinions about any topic, often with little or no information. They do not just express disagreement. They launch ad hominem attacks unrestricted by truth or morality. They make threats, spread fake stories and even attack your relatives.”

Rosenstein has maintained a tenuous relationship with Trump. Congressional Republicans have also accused him of withholding documents and not investigating aggressively enough what they contend was political bias within the FBI.

Former FBI General Counsel James Baker, in closed-door testimony before congressional committees last October, provided detail about internal discussions concerning Rosenstein's reported offer to wear a wire to tape the president in the tumultuous days following James Comey's firing as FBI director in May 2017.

Fox News has confirmed portions of the transcript to the House Oversight and Judiciary Committees.

"At my confirmation hearing in March 2017, a Republican senator asked me to make a commitment," he recalled. "He said: 'You're going to be in charge of this [Russia] investigation. I want you to look me in the eye and tell me that you'll do it right, that you'll take it to its conclusion and you'll report [your results] to the American people.'

"I did pledge to do it right and take it to the appropriate conclusion. I did not promise to report all results to the public, because grand jury investigations are ex parte proceedings. It is not our job to render conclusive factual findings. We just decide whether it is appropriate to file criminal charges."

Rosenstein is leaving his post in two months. He had some fun with his speech and answered the question that so many on social media were asking after watching him standing stoically behind Attorney General William Barr during the lead-up to the Mueller report release.

"Last week, the big topic of discussion was, 'What were you thinking when you stood behind Bill Barr at that press conference, with a deadpan expression?' The answer is: I was thinking, 'My job is to stand here with a deadpan expression.'"

[Deputy AG Rod Rosenstein offers staunch defense of Russia investigation, jabs Obama administration](#) USA Today

Deputy Attorney General Rod Rosenstein offered a staunch defense of the Justice Department's oversight of special counsel Robert Mueller's investigation late Thursday, claiming that evidence of Russia's election interference campaign represented "only the tip of the iceberg" in the Kremlin's strategy to undermine the American political system.

A week after a redacted version of Mueller's investigative report was made public, Rosenstein, who oversaw much of the investigation following the 2017 recusal of then-Attorney General Jeff Sessions, told an Armenian Bar Association gathering in New York that he only pledged to bring the investigation to "the appropriate conclusion."

"I did not promise to report all results to the public, because grand jury investigations are (secret) proceedings," according to Rosenstein's written remarks. "It is not our job to render conclusive factual findings. We just decide whether it is appropriate to file criminal charges."

Rosenstein's remarks come as Democratic lawmakers are demanding access to the unredacted version of Mueller's report, which found insufficient evidence that the Trump campaign and Russia engaged in a conspiracy to tilt the 2016 election to President Donald Trump.

Mueller's team did not reach a conclusion on whether Trump obstructed the investigation, but Attorney General William Barr and Rosenstein decided that there was insufficient evidence to support such a finding.

Democrats have seized on the decision by Barr and Rosenstein, suggesting that their intervention was inappropriate and that a final decision on obstruction should have been left to Congress to decide.

Rosenstein, who is set to leave the Justice Department next month, also claimed that critical decisions about the course of the investigation had been made before he took office exactly two years ago.

"The previous (Obama) administration chose not to publicize the full story about Russian computer hackers and social media trolls, and how they relate to a broader strategy to undermine America," Rosenstein said, adding that the FBI later disclosed classified evidence about the investigation to ranking legislators and their staffers only to have details "selectively" leaked to reporters.

A month before taking office, Rosenstein said then-FBI Director James Comey revealed the existence of the counterintelligence investigation at a congressional hearing and later alleged that the president "had pressured him to close the investigation."



"So that happened," Rosenstein said, suggesting that he was thrust into an already politically charged position.

"There is a story about firefighters who found a man on a burning bed. When they asked how the fire started, he replied, 'I don't know. It was on fire when I lay down on it.' I know the feeling," he said.

But Rosenstein said the baseline conclusion that Russia had interfered in the election was undeniable.

"There was overwhelming evidence that Russian operatives hacked American computers and defrauded American citizens, and that is only the tip of the iceberg of a comprehensive Russian strategy to influence elections, promote social discord, and undermine America, just like they do in many other countries," he said.

[Rosenstein Lashes Out at Obama and the Media, Defends Trump in First Remarks Since Mueller Report](#) Daily Beast

Speaking publicly for the first time since the release of Special Counsel Robert Mueller's report into Russian meddling in the 2016 presidential elections, Assistant Attorney General Rob Rosenstein did not mince words.

In a prepared speech delivered to the Public Servants Dinner of the Armenian Bar Association, Rosenstein criticized the Obama administration for failing to act on what he says should have been a "real-time reaction to Russian hacking."

"The previous Administration chose not to publicize the full story about Russian computer hackers and social media trolls, and how they relate to a broader strategy to undermine America," he said.

But he saved his harshest criticism for the press, which he accused of blatantly sensationalizing the facts surrounding his involvement in the two-year inquiry. "Some of the nonsense that passes for breaking news today would not be worth the paper it was printed on, if anybody bothered to print it," he said. "One silly question that I get from reporters is, 'Is it true that you got angry and emotional a few times over the past few years?' Heck yes! Didn't you?"

Rosenstein answered critics who say that he was complicit in what many believe was Attorney General William Barr's filtering of the report. "I did pledge to do it right and take it to the appropriate conclusion," he told those gathered. "I did not promise to report all results to the public, because grand jury investigations are ex parte proceedings. It is not our job to render conclusive factual findings. We just decide whether it is appropriate to file criminal charges."

Then he went further, addressing widespread criticism that he stood emotionless as Barr delivered remarks at a press conference the morning the redacted report was released. "Can you imagine if I did anything other than stand there at the press conference?" he asked. "Imagine the reaction and the commentary if I had smiled or grimaced. But you cannot avoid criticism. The only way you can avoid criticism in public service is if you stay home."

He only mentioned Trump once in the talk, praising the president's approach to the law. "The rule of law is our most important principle," Rosenstein said. "As President Trump pointed out, 'We govern ourselves in accordance with the rule of law rather [than] ... the whims of an elite few or the dictates of collective will.'"

Rosenstein warned that the Russian meddling outlined in the Mueller report was just the beginning.

"The bottom line is, there was overwhelming evidence that Russian operatives hacked American computers and defrauded American citizens," he said, according to the official transcript of the speech. "And that is only the tip of the iceberg of a comprehensive Russian strategy to influence elections, promote social discord, and undermine America, just like they do in many other countries."

[Rod Rosenstein Defends Handling Of Mueller Report](#) Daily Caller

Deputy Attorney General Rod Rosenstein spoke out Thursday night on special counsel Robert Mueller's report for the first time since its release.

At an official Justice Department dinner in New York hosted by the Armenian Bar Association, the embattled deputy attorney general reflected on his time in the Justice Department.

Rosenstein defended his handling of the special counsel's investigation, ripped former FBI Director James Comey and accused the Obama administration of misleading the American people on Russia.

"I did pledge to do it right and take it to the appropriate conclusion. I did not promise to report all results to the public because grand jury investigations are ex parte proceedings," Rosenstein said of Mueller's report, which found no evidence of collusion between the presidential campaign of Donald Trump and Russia.

"It is not our job to render conclusive factual findings," he continued. "We just decide whether it is appropriate to file criminal charges."

The deputy attorney general also took the time to slam the Obama administration for its handling of Russian meddling and the subsequent investigation: "The previous administration chose not to publicize the full story about Russian computer hackers and social media trolls, and how they relate to a broader strategy to undermine America."

He then discussed Comey's handling of the investigation, making clear that he was not happy with the former FBI director's handling of the investigation, saying:

The FBI disclosed classified evidence about the investigation to ranking legislators and their staffers. Someone selectively leaked details to the news media. The FBI director [Comey] announced at a congressional hearing that there was a counterintelligence investigation that might result in criminal charges. Then the former FBI director alleged that the president pressured him to close the investigation, and the president denied that the conversation occurred.

Rosenstein has previously defended Attorney General Bill Barr and the Justice Department's handling of the Mueller report, saying that Barr was being "as forthcoming as he can."

---

**From:** (b) (6) . (ODAG)  
**Sent:** Friday, April 26, 2019 6:13 PM  
**To:** Rosenstein, Rod (ODAG)  
**Subject:** Letter  
**Attachments:** 2019.04.26 Letter.docx

Good afternoon,

The soft copy is attached.

(b) (6)  
Special Assistant  
Office of the Deputy Attorney General  
Phone (b) (6)

---

**From:** (b) (6) . (ODAG)  
**Sent:** Monday, April 29, 2019 1:59 PM  
**To:** Rosenstein, Rod (ODAG)  
**Subject:** Final Draft  
**Attachments:** 2019.04.29 Resignation Letter.pdf

Good afternoon,

Your scanned letter is attached.

(b) (6)  
Special Assistant  
Office of the Deputy Attorney General  
Phone (b) (6)



Office of the Deputy Attorney General  
Washington, D.C. 20530

April 29, 2019

Dear Mr. President:

The Department of Justice made rapid progress in achieving the Administration's law enforcement priorities – reducing violent crime, curtailing opioid abuse, protecting consumers, improving immigration enforcement, and building confidence in the police – while preserving national security and strengthening federal efforts in other areas. We staffed the Department of Justice and the U.S. Attorneys' Offices with skilled and principled leaders devoted to the values that make America great. By consulting stakeholders, implementing constructive policies, reducing bureaucracy, and using results-driven management, we maximized the public benefit of our \$28 billion budget. Productivity rose, and crime fell.

Our nation is safer, our elections are more secure, and our citizens are better informed about covert foreign influence efforts and schemes to commit fraud, steal intellectual property, and launch cyberattacks. We also pursued illegal leaks, investigated credible allegations of employee misconduct, and accommodated congressional oversight without compromising law enforcement interests. I commend our 115,000 employees for their accomplishments and their devotion to duty. As Thomas Paine wrote, "Those who expect to reap the blessings of freedom must undergo the fatigues of supporting it."

The median tenure of a Deputy Attorney General is 16 months, and few serve longer than two years. As I submit my resignation effective on May 11, I am grateful to you for the opportunity to serve; for the courtesy and humor you often display in our personal conversations; and for the goals you set in your inaugural address: patriotism, unity, safety, education, and prosperity, because "a nation exists to serve its citizens." The Department of Justice pursues those goals while operating in accordance with the rule of law. The rule of law is the foundation of America. It secures our freedom, allows our citizens to flourish, and enables our nation to serve as a model of liberty and justice for all.

At the Department of Justice, we stand watch over what Attorney General Robert Jackson called "the inner ramparts of our society – the Constitution, its guarantees, our freedoms and the supremacy of law." As a result, the Department bears a special responsibility to avoid partisanship. Political considerations may influence policy choices, but neutral principles must drive decisions about individual cases. In 1940, Jackson explained that government lawyers "must at times risk ourselves and our records to defend our legal processes from discredit, and to maintain a dispassionate, disinterested, and impartial enforcement of the law." Facing "corrosive skepticism and cynicism concerning the administration of justice" in 1975, Edward Levi urged us to "make clear by word and deed that our law is not an instrument of partisan purpose, and it is not ... to be used in ways which are careless of the higher values ... within us all." In 2001, John Ashcroft called for "a professional Justice Department ... free from politics ... uncompromisingly fair ... defined by integrity and dedicated to upholding the rule of law."

We enforce the law without fear or favor because credible evidence is not partisan, and truth is not determined by opinion polls. We ignore fleeting distractions and focus our attention on the things that matter, because a republic that endures is not governed by the news cycle.

We keep the faith, we follow the rules, and we always put America first.

Sincerely,

A handwritten signature in blue ink, which appears to read "Rod J. Rosenstein", is written over a horizontal line.

Rod J. Rosenstein



---

**From:** Rosenstein, Rod (ODAG)  
**Sent:** Monday, April 29, 2019 3:40 PM  
**To:** Kupec, Kerri (OPA); O'Callaghan, Edward C. (ODAG); Ellis, Corey F. (ODAG); Peterson, Andrew (ODAG)  
**Cc:** Rabbitt, Brian (OAG)  
**Subject:** Resignation letter  
**Attachments:** 2019.04.29 Resignation Letter.pdf; ATT00001.htm

I just gave this letter to the President setting next Friday, May 10 as my last day. I told him that w (b) (5)  
(b) (5). He told me that we shoul (b) (5)  
(b) (5)

Kerri - Pleas (b) (5)

---

**From:** Carrie Johnson (b) (6) >  
**Sent:** Monday, April 29, 2019 7:35 PM  
**To:** Rosenstein, Rod (ODAG)  
**Subject:** Re: Off the record

Sorry I didn't get back to you on Friday about this. I wa (b) (6) [REDACTED], right when it arrived in my in-box, and then stuck in the airport for hours on weather delay.

In case you want to talk (before or after May 11), I'm a (b) (6) [REDACTED] office o (b) (6) [REDACTED] personal cell.

Carrie

Sent from my iPhone

On Apr 26, 2019, at 4:52 PM, Rosenstein, Rod (ODAG) (b) (6) [REDACTED] > wrote:

Here is a piece by a writer who construed my critique of "mercenary critics" to include reporters. Do they no longer distinguish real journalists from celebrity pundits?

<https://slate.com/news-and-politics/2019/04/rod-rostein-donald-trump-channeling-anti-media-speech.html>

On Apr 26, 2019, at 2:20 PM, Carrie Johnson (b) (6) [REDACTED] > wrote:

You? Never!

Looking forward to a sit-down when you have time.

Carrie

Sent from my iPhone

On Apr 26, 2019, at 2:17 PM, Rosenstein, Rod (ODAG) (b) (6) [REDACTED] > wrote:

I look forward to being able to speak freely to honest reporters without any minders. (But I still won't leak sensitive information!)

On Apr 26, 2019, at 9:25 AM, Carrie Johnson (b) (6) [REDACTED] > wrote:

Thank you for this. I appreciate it. I know that you have been an advocate of journalism that matters. Hoping that we can continue this conversation when you finally get a rest next month.

Carrie

Sent from my iPhone

On Apr 26, 2019, at 9:16 AM,  
Rosenstein, Rod (ODAG)

(b) (6) >  
wrote:

I saw one of your tweets. I hope the prepared remarks did not read as a criticism of “reporters” in general, or even particular individual reporters. I think my full remarks made clear that my complaint about “nonsense that passes for breaking news” refers to stories that are based on biased sources or that hype irrelevant matters.

---

**From:** Hiatt, Fred (b) (6) >  
**Sent:** Wednesday, May 1, 2019 4:56 PM  
**To:** Rosenstein, Rod (ODAG)  
**Subject:** RE: Off the record

Deal. Thanks.

---

**From:** Rosenstein, Rod (ODAG) (b) (6) >  
**Sent:** Tuesday, April 30, 2019 6:14 PM  
**To:** Hiatt, Fred (b) (6) >  
**Subject:** RE: Off the record

OK, as long as you agree not to use it until after I leave DOJ:

(b) (6)

---

**From:** Hiatt, Fred (b) (6) >  
**Sent:** Tuesday, April 30, 2019 12:07 PM  
**To:** Rosenstein, Rod (ODAG) (b) (6) >  
**Subject:** RE: Off the record

Rod,

I know you may not want to write anything after your now official resignation. But... would you share an email address where I could reach you, just in case?

Fred

---

**From:** Rosenstein, Rod (ODAG) (b) (6) >  
**Sent:** Friday, April 26, 2019 6:37 PM  
**To:** Hiatt, Fred (b) (6) >  
**Subject:** RE: Off the record

LOL

---

**From:** Hiatt, Fred (b) (6) >  
**Sent:** Friday, April 26, 2019 6:36 PM  
**To:** Rosenstein, Rod (ODAG) (b) (6) >  
**Subject:** RE: Off the record

As far as you know.

---

**From:** Rosenstein, Rod (ODAG) (b) (6) >  
**Sent:** Friday, April 26, 2019 6:25 PM  
**To:** Hiatt, Fred (b) (6) >  
**Subject:** RE: Off the record

Thanks! Too bad nobody was wearing a wire....

---

**From:** Hiatt, Fred (b) (6) >  
**Sent:** Friday, April 26, 2019 6:24 PM  
**To:** Rosenstein, Rod (ODAG) (b) (6) >  
**Subject:** RE: Off the record

Yes. I have relayed the message to a competent authority. It would seem to hinge on what was meant by "offering their own characterization of the call." I don't know if there will be any change, but I feel confident the editor will give the point serious consideration.  
F.

---

**From:** Rosenstein, Rod (ODAG) (b) (6) >  
**Sent:** Friday, April 26, 2019 6:15 PM  
**To:** Hiatt, Fred (b) (6) >  
**Subject:** RE: Off the record

Thanks! Not a big deal, but I understand it is creating a lot of secondary hoopla among the pundits. Even when we have credible witnesses who don't demand anonymity, we always try to clarify whether their hearsay recollections are actually the words the speaker used or merely the impressions that the witness formed.

---

**From:** Hiatt, Fred (b) (6) >  
**Sent:** Friday, April 26, 2019 6:08 PM  
**To:** Rosenstein, Rod (ODAG) (b) (6) >  
**Subject:** RE: Off the record

Rod,  
As you know, I don't oversee news coverage, but I will walk this over to someone who does now. You are right that things should not be in quotes unless a reporter is confident it is a direct quote.  
Fred

---

**From:** Rosenstein, Rod (ODAG) (b) (6) >  
**Sent:** Friday, April 26, 2019 5:57 PM  
**To:** Hiatt, Fred (b) (6) >  
**Subject:** Off the record

---

**CAUTION: EXTERNAL SENDER**

---

I rarely quibble about newspaper articles, but I request that you ask the appropriate person to review the language in the Zapotosky story that posted on the internet a few hours ago to confirm whether it meets Post editing standards.

If a credible source claims that I said the words, "I can land the plane," and "I give the investigation credibility," then so be it. But if the source actually was just characterizing what I supposedly said – i.e., what the source thinks I meant, or what somebody told the source – then it is misleading to headline the article with a quotation, and to attribute those specific words to me with the verb "said."

I don't claim to recall every word I have used in the past two years, but neither one of those quotes sounds like me. They sound more like people talking about me when I am not in the room. If your source says it was me, then so be it. But if your source does not say that, the article should make clear that they are NOT my words. Incidentally, if the source is truthful, why would he require anonymity about this?

“I give the investigation credibility,” Rosenstein said, in the words of one administration official offering their own characterization of the call. “I can land the plane.”



**Boyd, Stephen E. (OLA)**

---

**From:** Boyd, Stephen E. (OLA)  
**Sent:** Thursday, May 2, 2019 10:04 AM  
**To:** Rosenstein, Rod (ODAG)  
**Subject:** Fwd: Letter to Inspector General Horowitz and Director Amundson  
**Attachments:** 2019.04.30 Letter to DOJ OIG and OPR.pdf; ATT00001.htm

Sent from my iPhone

Begin forwarded message:

**From:** "Weinsheimer, Bradley (ODAG)" <(b) (6)>  
**Date:** April 30, 2019 at 5:53:38 PM EDT  
**To:** "Boyd, Stephen E. (OLA)" <(b) (6)>, "O'Callaghan, Edward C. (ODAG)" <(b) (6)>  
**Subject:** FW: Letter to Inspector General Horowitz and Director Amundson

FYSA. Brad.

---

**From:** Amundson, Corey (OPR) <(b) (6)>  
**Sent:** Tuesday, April 30, 2019 4:56 PM  
**To:** Weinsheimer, Bradley (ODAG) <(b) (6)>; Ragsdale, Jeffrey (OPR) <(b) (6)>  
**Subject:** FW: Letter to Inspector General Horowitz and Director Amundson

FYI

---

**From:** Berger, Christine (Judiciary-Dem)  
**Sent:** Tuesday, April 30, 2019 1:11 PM  
**To:** 'Lee, Rene R. (OIG)' <(b) (6)>; 'Miles, Adam (OIG)' <(b) (6)>; (b)(6) per OIG (OIG) <(b) (6)>; 'opr.complaints@usdoj.gov' <opr.complaints@usdoj.gov>  
**Cc:** Greenfeld, Helaine (Hirono) <(b) (6)>  
**Subject:** Letter to Inspector General Horowitz and Director Amundson

Dear all,

Please find attached a copy of a letter sent by mail to Inspector General Horowitz and Director Amundson from Senators Mazie Hirono, Richard Blumenthal, Kamala D. Harris, Edward J. Markey, Tom Udall, Ron Wyden, Sheldon Whitehouse, Patty Murray, Cory A. Booker, Jack Reed, Kristen Gillibrand, and Amy Klobuchar.

Best regards,  
Christine

***Christine Berger***

*Senior Counsel*

Office of Senator Mazie Hirono | Committee on the Judiciary

713 Hart Senate Office Bldg. Washington, DC 20510

(b) (6)

# United States Senate

WASHINGTON, DC 20510

April 30, 2019

The Honorable Michael E. Horowitz  
Inspector General  
U.S. Department of Justice  
950 Pennsylvania Avenue, NW  
Washington, D.C. 20530

Corey R. Amundson  
Director and Chief Counsel  
Office of Professional Responsibility  
U.S. Department of Justice  
950 Pennsylvania Avenue, NW, Suite 3266  
Washington, D.C. 20530

Dear Inspector General Horowitz and Director Amundson:

We write regarding the serious concerns that have been raised about the actions of Attorney General William Barr with respect to his handling of Special Counsel Robert Mueller's report. Attorney General Barr's actions raise significant questions about his decision not to recuse himself from overseeing the Special Counsel's investigation, whether his actions with respect to the release of the report complied with Department of Justice policies and practices, and whether he has demonstrated sufficient impartiality to continue overseeing the fourteen criminal matters related to the Special Counsel's investigation that were referred principally to other components of the Department of Justice and the Federal Bureau of Investigation (FBI).<sup>1</sup> In light of these concerns, we respectfully request that the Office of the Inspector General and the Office of Professional Responsibility immediately begin investigations of these issues.

Six months before his nomination to be Attorney General, Mr. Barr wrote an unsolicited 19-page memo to Deputy Attorney General Rod Rosenstein and Assistant Attorney General for the Office of Legal Counsel Steve Engel criticizing Special Counsel Mueller's investigation of obstruction of justice by Donald Trump.<sup>2</sup> In his memo, Mr. Barr conceded that he was "in the dark about many facts," and yet he asserted that "Mueller's obstruction theory is fatally misconceived" and premised on a "legally insupportable reading of the law."<sup>3</sup> Mr. Barr also argued that "Mueller should not be permitted to demand that the President submit to interrogation about alleged obstruction."<sup>4</sup> Despite this memo, which presents, at the very least, an appearance of bias, Mr. Barr refused to recuse himself from directly overseeing Special Counsel Mueller's investigation when he was confirmed as Attorney General.<sup>5</sup> While the Justice Department stated that Attorney General Barr's decision to not recuse was consistent with the advice of senior ethics attorneys, it provided few details about the nature of this seemingly anomalous decision. Given the Attorney General's subsequent troubling actions in handling the Special Counsel's report, further investigation of the process leading to his non-recusal decision is warranted.

---

<sup>1</sup> Department of Justice, *Report On The Investigation Into Russian Interference In The 2016 Presidential Election*, Appendix D, <https://www.justice.gov/storage/report.pdf>.

<sup>2</sup> Memo from Bill Barr to Deputy Attorney General Rod Rosenstein and Assistant Attorney General Steve Engel, June 8, 2018, available at <https://int.nyt.com/data/documenthelper/549-june-2018-barr-memo-to-doj-mue/b4c05e39318dd2d136b3/optimized/full.pdf#page=1>.

<sup>3</sup> *Id.* at 1.

<sup>4</sup> *Ibid.*

<sup>5</sup> See Josh Gerstein, *Barr won't recuse himself from Mueller oversight*, POLITICO (March 4, 2019), <https://www.politico.com/story/2019/03/04/barr-wont-recuse-mueller-1203210>.

Attorney General Barr's actions following the completion of Special Counsel Mueller's report raise further questions regarding his impartiality towards the Special Counsel's investigation and the appropriateness of his conduct as the chief law enforcement officer of the United States. After notifying Congress and the public on Friday, March 22, 2019, that he had received the Special Counsel's report,<sup>6</sup> Attorney General Barr released a four-page letter on March 24, 2019, that purported "to summarize the principal conclusions reached by the Special Counsel."<sup>7</sup> The letter, however, selectively quoted fragments from the Special Counsel's report. Moreover, the subsequent release of the redacted report revealed that the Attorney General's letter had presented quotations from the report out of context or with key words omitted to suggest that the President had been cleared of wrongdoing.<sup>8</sup> Given that the Special Counsel's report included executive summaries that seem to have been readily available for public release, we found the letter particularly concerning as a possible effort to mislead the public.

We are also troubled by the Attorney General's use of his March 24 letter to summarily conclude that the "evidence developed during the Special Counsel's investigation is not sufficient to establish that the President committed an obstruction-of-justice offense."<sup>9</sup> The letter asserts, without any justification, that the Special Counsel's decision not to reach "any legal conclusions leaves it to the Attorney General to determine whether the conduct described in the report constitutes a crime."<sup>10</sup> It is unclear what statute, regulation, or policy led the Attorney General to interject his own conclusion that the President's conduct did not amount to obstruction of justice, particularly when he had not yet released the redacted Special Counsel's report, which explicitly noted that "if we had confidence after a thorough investigation of the facts that the President clearly did not commit obstruction of justice, we would so state."<sup>11</sup> The Attorney General's conduct is even more concerning given that the report itself identifies Congress's impeachment authority and future prosecution once the President leaves office as possible ways to address the obstruction of justice evidence. But the report does not refer to a purported role of the Attorney General to make legal conclusions that the Special Counsel expressly declined to make.<sup>12</sup>

In addition, we found disturbing that Attorney General Barr provided the President's personal attorneys access to the Special Counsel's report before Congress and the public. News reports indicate that the Attorney General granted Rudy Giuliani, Jay Sekulow and two other Trump lawyers access to review the full redacted report for two days before providing the redacted report to Congress and the public.<sup>13</sup> While the Attorney General asserted that the President's personal attorneys' request to review the redacted report before its public release "was consistent with the practice followed under the Ethics in Government Act," we have serious concerns about

---

<sup>6</sup> Letter from Attorney General William Barr (March 22, 2019), available at <https://int.nyt.com/data/documenthelper/708-attorney-general-william-barr-letter-mueller/b7fd3a05ab618bad8544/optimized/full.pdf#page=1>.

<sup>7</sup> Letter from Attorney General William Barr (March 24, 2019), available at <https://www.documentcloud.org/documents/5779688-AG-March-24-2019-Letter-to-House-and-Senate.html>.

<sup>8</sup> See Charlie Savage, *How Barr's Excerpts Compare to the Mueller Report's Findings*, N.Y. TIMES (April 20, 2019), <https://www.nytimes.com/2019/04/19/us/politics/mueller-report-william-barr-excerpts.html>.

<sup>9</sup> *Supra* note 7.

<sup>10</sup> *Ibid.*

<sup>11</sup> *Supra* note 1, at vol. 2, p. 8.

<sup>12</sup> See, e.g., *supra* note 1, at vol. 2, p. 8, 178.

<sup>13</sup> See, e.g., Karen Freifeld, *Trump lawyers reviewed Mueller report for 10 hours before it was made public*, REUTERS (April 19, 2019), <https://www.reuters.com/article/us-usa-trump-russia-lawyers-idUSKCN1RV18M>.



the propriety of the Attorney General's decision to grant access to the full redacted report, particularly when he did not appear to grant other individuals named in the report similar access and he did not limit review to the portions of the report referencing Donald Trump.<sup>14</sup> This decision to purportedly act "consistent with the practice" under an expired law merits exacting review to determine whether the Attorney General's action was appropriate and justified, given that he ignored other provisions of this law, such as those requiring Congress to be provided with information necessary to enable it to conduct proper oversight.<sup>15</sup>

We further believe that Attorney General Barr's decision to hold a press conference to assert his own views regarding the report well before releasing the redacted report and his statements at the press conference warrant serious scrutiny as to whether they were proper and consistent with Justice Department policies and practices. At the press conference, Attorney General Barr appeared to make statements that were inconsistent with the Special Counsel's findings and demonstrated a lack of impartiality. For example, the Attorney General claimed that "the White House fully cooperated with the Special Counsel's investigation," despite the Special Counsel's detailed findings of President Trump's efforts to obstruct the investigation, refusal to be interviewed by the Special Counsel, and submission of "inadequate" written responses.<sup>16</sup> The Attorney General also repeatedly asserted that there was "no collusion," defending the President as "frustrated and angered by a sincere belief that the investigation was undermining his presidency."<sup>17</sup>

Moreover, the Attorney General's statements at the press conference compounded the misleading impression he created in his March 24 letter regarding the Special Counsel's determinations regarding the criminality of the President's conduct. In both his March 24 letter and his statements at the press conference, Attorney General Barr gave the misimpression that the guidelines from the Justice Department's Office of Legal Counsel (OLC) against indicting a sitting president played little to no role in the Special Counsel's decision to not charge the President with obstruction of justice.<sup>18</sup> The redacted report, however, makes clear that the OLC's guidelines played a significant role in the Special Counsel's decision, stating that the Special Counsel's office "accepted OLC's legal conclusion for the purpose of exercising prosecutorial jurisdiction."<sup>19</sup> These statements and actions, along with the Attorney General's prior statements, such as his claim that the federal government's investigation of the Trump campaign constituted "spying," also indicate that he lacks the impartiality to continue overseeing ongoing matters stemming from the Special Counsel's investigation.<sup>20</sup>

---

<sup>14</sup> Attorney General William P. Barr Delivers Remarks on the Release of the Report on the Investigation into Russian Interference in the 2016 Presidential Election, April 18, 2019, <https://www.justice.gov/opa/speech/attorney-general-william-p-barr-delivers-remarks-release-report-investigation-russian>.

<sup>15</sup> See, e.g., 28 U.S.C. 595(c); 28 U.S.C. 594(h).

<sup>16</sup> Compare *ibid.* with *supra* note 1, Appendix C.

<sup>17</sup> *Supra* note 15.

<sup>18</sup> Aaron Blake, *How William Barr successfully pre-spun the Mueller report for Trump*, N.Y. TIMES (April 19, 2019), [https://www.washingtonpost.com/politics/2019/04/19/how-william-barr-successfully-pre-spun-mueller-report-trump/?utm\\_term=.122c1c6362ba](https://www.washingtonpost.com/politics/2019/04/19/how-william-barr-successfully-pre-spun-mueller-report-trump/?utm_term=.122c1c6362ba).

<sup>19</sup> *Supra* note 1, at vol. 1, p. 1.

<sup>20</sup> See, e.g., Nicholas Fandos and Adam Goldman, *Barr Asserts Intelligence Agencies Spied on the Trump Campaign*, N.Y. TIMES (April 10, 2019), <https://www.nytimes.com/2019/04/10/us/politics/barr-trump-campaign-spying.html>.

Given these concerns, we therefore urge the Office of the Inspector General and the Office of Professional Responsibility to initiate immediately investigations of the following matters:

- Whether Attorney General Barr's decision not to recuse himself from overseeing the Special Counsel's investigation was proper and consistent with ethical rules and practices within the Department of Justice;
- Whether Attorney General Barr's four-page letter dated March 24, 2019, regarding Special Counsel Mueller's report was misleading and whether it was consistent with Department of Justice policies and practices;
- Whether Attorney General Barr's actions in permitting President Trump's private attorneys to review the entire Special Counsel's report at length before sharing the report with Congress, other individuals named in the report, and the public, was appropriate and consistent with Department of Justice policies and practices;
- Whether Attorney General Barr's press conference on April 18, 2019, regarding Special Counsel Mueller's report, which took place well before he released a redacted version of the report, was misleading and consistent with Department of Justice policies and practices;
- Whether Attorney General Barr has demonstrated sufficient impartiality to continue overseeing the ongoing matters related to the Special Counsel's investigation referenced in Appendix D of the Special Counsel's report;
- Whether Attorney General Barr took any steps related to the transfers and referrals listed in Appendix D of the report that were contrary to the advice of career prosecutors at the Justice Department or the Department's policies; and
- Whether any of Attorney General Barr's other actions or statements call into question his impartiality such that they warrant his recusal from particular matters or are relevant to the Senate Judiciary Committee's oversight into the Department of Justice.

Thank you for your consideration of this important matter. We look forward to a prompt response.

Sincerely,



MAZIE K. HIRONO  
United States Senator



RICHARD BLUMENTHAL  
United States Senator



KAMALA D. HARRIS  
United States Senator



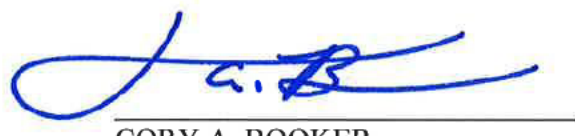
EDWARD J. MARKEY  
United States Senator

  
TOM UDALL  
United States Senator

  
RON WYDEN  
United States Senator

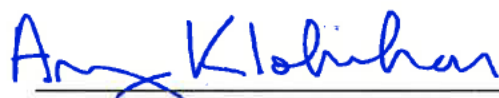
  
SHELDON WHITEHOUSE  
United States Senator

  
PATTY MURRAY  
United States Senator

  
CORY A. BOOKER  
United States Senator

  
JACK REED  
United States Senator

  
KIRSTEN GILLIBRAND  
United States Senator

  
AMY KLOBUCHAR  
United States Senator



---

**From:** Gurman, Sadie (b) (6) >  
**Sent:** Thursday, May 2, 2019 11:39 AM  
**To:** Rosenstein, Rod (ODAG)  
**Subject:** Re: The story, and thank you

Of course. As long as you promise to respond to it after May 12!

Sadie Gurman  
WASHINGTON BUREAU  
<http://www.wsj.com/>  
**O** (b) (6) | **M** (b) (6)  
**E** (b) (6) | **T:** [@sgurman](mailto:@sgurman)  
**A:** [1025 Connecticut Ave. NW, Suite 800 | Washington, D.C. 20036](#)  
<http://www.dowjones.com/>  
Sign up for WSJ's free Capital Journal newsletter [here](#).

On Thu, May 2, 2019 at 11:23 AM Rosenstein, Rod (ODAG) (b) (6) > wrote:

As long as you promise not to use it before May 12:

(b) (6)

**From:** Gurman, Sadie (b) (6) >  
**Sent:** Thursday, May 2, 2019 10:16 AM  
**To:** Rosenstein, Rod (ODAG) (b) (6) >  
**Subject:** Re: The story, and thank you

Rod,

I hope you are well. What's the best way to reach you at a non-DOJ email address? I promise I will not abuse or share it.

Sadie Gurman

**WASHINGTON BUREAU**

<http://www.wsj.com/>

O (b) (6) | M (b) (6)

E (b) (6) | T: [@sgurman](#)

A: [1025 Connecticut Ave. NW, Suite 800 | Washington, D.C. 20036](#)

<http://www.dowjones.com/>

Sign up for WSJ's free Capital Journal newsletter [here](#).

On Tue, Apr 23, 2019 at 11:00 AM Gurman, Sadie (b) (6) > wrote:

That makes sense. I will quibble with your point about reporters some other time! But I see what you are saying.

I have heard you were surprised that Mueller did not make a recommendation on the obstruction question. Given all of this, do you think he could and should have reached a conclusion?

Sadie Gurman

**WASHINGTON BUREAU**

<http://www.wsj.com/>

O (b) (6) | M (b) (6)

E (b) (6) | T: [@sgurman](#)

A: [1025 Connecticut Ave. NW, Suite 800 | Washington, D.C. 20036](#)

<http://www.dowjones.com/>

Sign up for WSJ's free Capital Journal newsletter [here](#).

On Mon, Apr 22, 2019 at 7:25 PM Rosenstein, Rod (ODAG) (b) (6) >  
wrote:

Off the record:

My public comments acknowledged that there may be legitimate reasons to make exceptions. My point is that if you charge a case, the public finds out whether you were correct in believing that you had sufficient credible evidence to prove the defendant guilty of every legal element of the crime beyond any reasonable doubt to the satisfaction of a judge and a jury of 12 random citizens. (Then people just argue about whether the case satisfied the principles of federal prosecution.) If you do not charge the case, people can always argue about the strength of any untested evidence.

In contrast – not a criticism, just a fact – reporters can run a story if there is one anonymous hearsay witness of unknown credibility. Politicians need no witnesses at all. There are different standards of proof in different lines of work. Mine is the highest.

**From:** Gurman, Sadie (b) (6) >  
**Sent:** Monday, April 22, 2019 4:36 PM  
**To:** Rosenstein, Rod (ODAG) (b) (6) >  
**Subject:** Re: The story, and thank you

Very interesting – yes, I remember you have spoken about this quite a bit. Thank you for pointing me to these. Should I read this to mean, then, that you disagreed with the AG's decision to release the full report because of all of the derogatory information it contains about someone who was ultimately not charged with a crime?

Sadie Gurman

**WASHINGTON BUREAU**

<http://www.wsj.com/>

O (b) (6) | M (b) (6)

E (b) (6) | T: [@sgurman](#)

A: [1025 Connecticut Ave. NW, Suite 800 | Washington, D.C. 20036](#)

<http://www.dowjones.com/>

Sign up for WSJ's free Capital Journal newsletter [here](#).

On Mon, Apr 22, 2019 at 3:45 PM Rosenstein, Rod (ODAG)

(b) (6) > wrote:

Off the record:

I think the AG said at the press conference that the Special Counsel's found substantial evidence that the President was frustrated; not that it is dispositive of whether there was a crime.

Re my analysis, I do not regard it as my job to express a definitive conclusion about factual issues in cases we do not prosecute.

<https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-associated-alumni-central-high>

The need to prove our claims in court imposes a powerful discipline on prosecutors. When we file a criminal allegation, the defendant is presumed innocent. We need to introduce sufficient credible evidence to satisfy a judge and prove our case beyond any reasonable doubt to the unanimous satisfaction of a jury of 12 random citizens. The government must disclose any exculpatory evidence, and the defendant may cross-examine our witnesses and offer his own evidence. Even if the defendant remains silent, the court presumes him innocent. If any single juror is not persuaded beyond a reasonable doubt, the defendant goes free.

Sometimes people look at our high conviction rates and mistakenly assume that the job is easy. But the opposite is true. Conviction rates are high because federal prosecutors exercise great care before we accuse anyone of wrongdoing. The scrutiny makes us appropriately cautious.

<https://www.csis.org/analysis/defending-rule-law-norms-conversation-rod-rosenstein>

One of the challenging issues we face in the department – and this is an issue that, you know, we’ll be discussing nationally – is the question of whether transparency is a good thing. You know, there’s a knee-jerk reaction that suggests that we should be transparent about what we do in government, but there are a lot of reasons not to be transparent about what we do in government. Judge Webster is sitting here in the front row. He’s been doing this work since long before I. You know, the government – just because the government collects information doesn’t mean that information is accurate, and it can be really misleading if you’re overly transparent about information that the government collects. So I think we do need to be really cautious about that.

And that’s, again, not to comment on any particular case. There may be legitimate reasons for making exceptions. But as a general principle, you know, my view is the Department of Justice is best served when people are confident that we’re going to operate – when we’re investigating American citizens in particular, we’re going to do it with appropriate sensitivity to the rights of uncharged people.

And as I mentioned in my remarks, when we charge somebody with a violation, we need to be prepared to prove it by evidence beyond any reasonable doubt. And, you know, the guidance I always gave my prosecutors and the agents that I worked with during my tenure on the front lines of law enforcement [was that] if we aren’t prepared to prove our case beyond a reasonable doubt in court, then we have no business making allegations against American citizens.

So I know there’s tension there between the desire to be more transparent and let everybody know what we’re doing and the desire to ensure the government, through its work, is not unduly tainting anybody. But my own view about it is that we’re better off following the rules and ensuring that our employees respect their obligations to conduct their investigations in confidence.

Also see page 182 of the Bharara book.

**From:** Gurman, Sadie (b) (6) >

**Sent:** Monday, April 22, 2019 3:06 PM

**To:** Rosenstein, Rod (ODAG) (b) (6) >  
**Subject:** Re: The story, and thank you

Thank you for your quick response! I understand it is off the record, and I will honor that. A good point about him giving people the opportunity to draw their own conclusions -- the public could conceivably ignore the speech and read the report.

I guess what I still wonder is if you share the opinions that the attorney general voiced at the press conference -- specifically his point that the president's actions that were under investigation were an expression of his frustration, rather than a crime. Would that be your analysis as well?

And again, thank you for getting back to me.

Sadie Gurman

**WASHINGTON BUREAU**

<http://www.wsj.com/>

**O** (b) (6) | **M** (b) (6)

**E** (b) (6) | **T:** [@sgurman](#)

**A:** [1025 Connecticut Ave. NW, Suite 800 | Washington, D.C. 20036](#)

<http://www.dowjones.com/>

Sign up for WSJ's free Capital Journal newsletter [here](#).

On Mon, Apr 22, 2019 at 2:48 PM Rosenstein, Rod (ODAG)  
(b) (6) > wrote:

You will need to check with OPA for any fresh quotes from me.

Off the record:

Your use of “forthcoming as he could be” below may be out of context; I don’t think I said that the letter alone was forthcoming. My point was that AG Barr decided that he was going to release the entire report TO THE PUBLIC with only reasonable and necessary redactions IDENTIFIED BY THE SPECIAL COUNSEL, thereby allowing people to draw their own conclusions, so they do not need to rely on his (or my) opinion. What more could anyone ask for? That is when I meant by saying that he decided to be as forthcoming as he could be.

Regarding the letter, the AG decided that it was not feasible to keep everybody in the dark about the conclusions for the few weeks that it would take to produce a redacted version.

I think I correctly forecasted for you that people would find fault with the “principal conclusions” letter if they treated it as if it were a summary of the report; it does not purport to summarize the facts. But the big picture point is: when he committed to release the report with no privilege redactions – which was really a remarkable decision – obviously he was not planning to mislead people. Same goes for the press conference. The AG disclosed the facts. People are free to disagree with his opinions.

**From:** Gurman, Sadie (b) (6) >  
**Sent:** Monday, April 22, 2019 1:02 PM  
**To:** Rosenstein, Rod (ODAG) (b) (6) >  
**Subject:** Re: The story, and thank you

Hi, Rod,

I hope you are well and that you were able to take your vacation! Just wanted to circle back to you now that the report is out to see how you are doing and to see if I can get your thoughts on how it all went down. The AG has been pretty harshly criticized for his news conference and summaries of the report -- do you still stand by your defense of his handling of things and believe he was as forthcoming as he could be? Would love to hear your take on the situation, even totally off the record. Reachable always a (b) (6) and still just three floors away.



Sadie Gurman

**WASHINGTON BUREAU**

<http://www.wsj.com/>

**O** (b) (6) | **M** (b) (6)

**E** (b) (6) | **T:** [@sgurman](#)

**A:** [1025 Connecticut Ave. NW, Suite 800 | Washington, D.C. 20036](#)

<http://www.dowjones.com/>

Sign up for WSJ's free Capital Journal newsletter [here](#).

On Fri, Apr 12, 2019 at 12:16 AM Rosenstein, Rod (ODAG)

(b) (6) > wrote:

You know where to find me!

On Apr 11, 2019, at 6:27 PM, Gurman, Sadie (b) (6) > wrote:

Rod,

I wanted to thank you again for taking the time to talk to me today and for your candor. Here is the story. I hope you find it an accurate reflection of our conversation: <https://www.wsj.com/articles/rod-rosenstein-defends-justice-department-handling-of-mueller-report-11555021002?mod=searchresults&page=1&pos=1>

Also, as we discussed, I will be holding onto your broader comments about morale and your work here for a story that will be timed more closely to your departure. I will circle back to Kerri as that story shapes up.

In the meantime, I would love to keep the conversation going, so please keep in touch.

Thank you again for your time and willingness to get together,

Sadie Gurman

**WASHINGTON BUREAU**

<http://www.wsj.com/>

**O** (b) (6) | **M** (b) (6)

**E** (b) (6) | **T:** [@sgurman](#)

**A:** [1025 Connecticut Ave. NW, Suite 800 | Washington, D.C. 20036](#)

<http://www.dowjones.com/>

Sign up for WSJ's free Capital Journal newsletter [here](#).

---

**From:** Ferguson, Andrew (Judiciary-Rep) (b) (6) >  
**Sent:** Friday, May 3, 2019 6:23 PM  
**To:** Ferguson, Andrew (Judiciary-Rep)  
**Subject:** Senate Judiciary Committee Update 4/29–5/3  
**Attachments:** SJC Status Update 5-2-19.pdf; 2019 Nominations Overview.pdf; Joseph Bianco Memo.pdf; Michael Park Memo.pdf

Hello, everybody. The Senate got back from a two-week recess and hit the century mark for judges!

1. The Senate this week confirmed the 100<sup>th</sup> Article III judge of the Trump presidency. On **May 1**, the Senate confirmed **J. Campbell Barker** to be a district judge for the Eastern District of Texas [by a party-line vote of 51-47](#), and **Andrew Brasher** to be a district judge for the Middle District of Alabama [by a party-line vote of 52-47](#). Both seats had been vacant since the middle of 2015. On **May 2**, the Senate confirmed the 100<sup>th</sup> Article III judge since President Trump took office: **Rodolfo Armando Ruiz II** to be a district judge in the Southern District of Florida [by a vote of 90-8](#). Not resting on its laurels, only minutes later the Senate confirmed two more district judges: **Raúl M. Arias-Marxuach** to the District of Puerto Rico [by a vote of 95-3](#), and **Joshua Wolson** to the Eastern District of Pennsylvania [by a vote of 65-33](#).

Here is where we stand. Under the leadership of Chairman Graham, Leader McConnell, and former Chairman Grassley, the Senate has confirmed 102 Article III judges since President Trump took office—2 Supreme Court Justice, 37 circuit judges, and 63 district judges. And those numbers are quickly going to rise. The Committee continues to churn out nominees. Under Chairman Graham, the Committee has sent 55 judicial nominees to the floor since February with plenty more on deck. And the Senate’s change to the cloture rule has broken the dam of Democrat obstruction and dramatically increased the rate at which the Senate can confirm district-judge nominees. The Senate has confirmed 10 district judges in the two and a half weeks it has been in session since the rules change. So, 102 confirmed judges is a significant milestone. But we have lots of work still to do in order to complete the transformation of the federal judiciary.

2. On **April 30**, Chairman Graham convened the [seventh nominations hearing](#) of the 116<sup>th</sup> Congress. Senator Cornyn presided. The Committee heard from four highly qualified nominees: **Ada Brown** to be a district judge for the Northern District of Texas, **Steven Grimberg** to be a district judge for the Northern District of Georgia, **David John Novak** to be a district judge for the Eastern District of Virginia, and **Matthew Solomson** to be a judge of the Court of Federal Claims. The Committee will vote on these nominees at a markup later in May.
3. On **May 2**, the Committee under Chairman Graham’s leadership [held a markup](#) to consider several nominations and bills. The Democrats [held over](#) the four judicial nominees on the agenda for the first time, as well as the Jeffrey Rosen, the President’s nominee to be U.S. Deputy Attorney General. The Committee will vote on those nominations [at its markup on May 9](#).

I must note that the Committee under Chairman Graham confirmed five district judges, held a hearing for four more, and held a markup while also holding [a day-long hearing on the Mueller Report](#). I’m sure most of you saw parts of that hearing or read the extensive news coverage, so I will say only that Chairman Graham allowed a full and fair evaluation of the Mueller Report by every member of the Judiciary Committee. And Attorney General William Barr—whom Chairman Graham guided to confirmation back in February—answered the hundreds of questions posed to him with a dignity and grace that, unfortunately, was not extended to him by the Democrats on the Committee.

4. On May 2, the Leader petitioned for cloture on two Second Circuit nominees—Judge Joseph Bianco and Michael Park. I’ve attached memos on both nominees. Chairman Graham [held a hearing](#) for these nominees on February 13, 2019, and reported them to the floor on March 7, 2019. Both are outstanding nominees, and have been rated Well Qualified by the ABA—which, according to the Democrats, is the “[gold standard by which judicial candidates are judged](#).” Judge Bianco was a counterterrorism prosecutor before President Bush made him a district judge in the Eastern District of New York in 2006. Mr. Park is a leading New York appellate lawyer who clerked for Justice Alito twice—once on the Third Circuit and again on the Supreme Court. Notwithstanding these nominees’ peerless credentials, Senators Schumer and Gillibrand have declined to return blue slips for either nominee because they oppose Mr. Park’s judicial philosophy. As I explained in my update on March 8, Senator Graham moved forward with their hearings because political objections to a judge’s philosophy are not acceptable grounds to withhold a blue slip. The Senate will vote on these nominees next week.

A quick further note on Senator Schumer’s refusal to return a blue slip for Judge Bianco. Senator Schumer unequivocally supported Judge Bianco’s nomination to the district court in 2006. At Judge Bianco’s 2005 confirmation hearing, Senator Schumer described Judge Bianco as a “great nominee[]” and as “high quality,” and said that he was “proud to support someone so outstandingly qualified and well respected as Mr. Bianco.” That his tune on Judge Bianco has changed so dramatically—when Judge Bianco’s qualifications have become only more impressive—is a testament to the mindless partisan rancor that characterizes the left’s opposition to President Trump’s nominees.

5. Finally, today the President [announced his intention to nominate](#) Judge Peter J. Phipps to the Third Circuit, as well as five new district-judge nominees. A quick word on Judge Phipps. President Trump nominated Judge Phipps to be a district judge in the Western District of Pennsylvania on February 15, 2018. The bipartisan nominating commission established by Senators Toomey and Casey had recommended Judge Phipps to the Senators, who had in turn recommended him to the White House. Both Senators returned blue slips for Judge Phipps’s nomination. Both Senators introduced Judge Phipps at his hearing on April 25, 2018. The Committee reported him to the floor by voice vote, and the Senate confirmed him by voice vote in October 2018.

**Andrew Ferguson**

Chief Counsel for Nominations and the Constitution

Senate Judiciary Committee

Chairman Lindsey Graham (R-South Carolina)



---

**From:** Leeman, Gabrielle (ODAG)  
**Sent:** Tuesday, May 7, 2019 10:18 AM  
**To:** Rosenstein, Rod (ODAG); O'Callaghan, Edward C. (ODAG); Ellis, Corey F. (ODAG); Peterson, Andrew (ODAG); Bacon, Antoinette T. (ODAG); Baughman, Matthew (ODAG); Braverman, Adam L. (ODAG); Cook, Steven H. (ODAG); Gauhar, Tashina (ODAG); Goldsmith, Andrew (ODAG); Groves, Brendan M. (ODAG); Harris, Stacie B. (ODAG); Hovakimian, Patrick (ODAG); Hughes, William C. (ODAG); Hunt, Ted (ODAG); Lan, Iris (ODAG); Liskamm, Amanda N. (ODAG); Masling, Mark (ODAG); Metcalf, David (ODAG); Michalic, Mark (ODAG); Perkins, Paul (ODAG); Raman, Sujit (ODAG); Weinsheimer, Bradley (ODAG); Wetmore, David H. (ODAG)  
**Cc:** Powell, SeLena Y (ODAG); Suero, Maya A. (ODAG); Heane, Kristen (ODAG)  
**Subject:** FOIA Update  
**Attachments:** Notification of Records Search to be Conducted in Response to the FOIA, Walker, OIP No. DOJ-2019-003300; Notification of Records Search to be Conducted in Response to the FOIA, Walker, OIP No. DOJ-2019-003327; Notification of Records Search to be Conducted in Response to the FOIA, Jason Leopold, OIP No. DOJ-2019- 003019 ; Notification of Records Search to be Conducted in Response to the FOIA, Rob Arthur, OIP No. DOJ-2019-003060; Notification of Records Search to be Conducted in Response to the FOIA, Leslie Gillispie, OIP No. DOJ-2019-003171 ; : Subject: Notification of Records Search to be Conducted in Response to the FOIA, Evers, OIP No. DOJ-2019-003895; Notification of Records Search to be Conducted in Response to the FOIA, Katelyn Polantz, OIP No. DOJ-2019-003237 ; Notification of Records Search to be Conducted in Response to the FOIA, John Greenewald, OIP No. DOJ-2019-003275 ; Notification of Records Search to be Conducted in Response to the FOIA, Katelyn Polantz, OIP No. DOJ-2019-003240 ; Notification of Records Search to be Conducted in Response to the FOIA, Katelyn Polantz, OIP No. DOJ-2019-003241 ; Notification of Records Search to be Conducted in Response to the FOIA, Katelyn Polantz, OIP No. DOJ-2019-003235 ; Notification of Records Search to be Conducted in Response to the FOIA, Paul Kamenar, OIP No. DOJ-2018-008172

Hi all,

Over the past few weeks, we received the attached 12 FOIA requests, which are also described below. Unless noted otherwise, the request will search the files of the DAG, all ODAG attorneys present during the relevant timeframe, SeLena, and Maya. Please let me know if you have any questions.

The requester, **Mark Walker of the New York Times**, is seeking:

- Email between Edward O'Callaghan and individuals currently or formerly with the United States Attorney's Office for the Southern District of New York - Robert Khuzami, Russell Capone, and Tatiana Martins.
- Timeframe: Since April 8, 2018.
- *The officials that will be searched for this request are: Edward O'Callaghan*

The requester, **Mark Walker of The New York Times**, is seeking:

- Records related to the merger of AT&T and Time Warner
- Timeframe: since October 1, 2016

The requester, **Jason Leopold**, is seeking:

- Records pertaining to discussions between former Federal Bureau of Investigation Acting Director McCabe and Deputy Attorney General Rosenstein (see attached request)
- Timeframe: February 1, 2017 - July 31, 2017

The requester, **Rob Arthur**, is seeking:

- Records pertaining to the review of consent decrees ordered by former Attorney General Sessions, pursuant to memorandum dated March 31, 2017 (see attached request)

The requester, **Leslie Gillispie**, is seeking:

- All records pertaining to the appointment of Special Counsel Robert S. Mueller, III

The requester, **Austin Evers of American Oversight**, is seeking:

- Various records of communication, including the White House, pertaining to the Attorney General William Barr's March 24, 2019 letter to the Senate and House Judiciary Committees regarding the investigation overseen by Special Counsel Robert Mueller
- Timeframe: March 1, 2019 through March 25, 2019

The requester, **Katelyn Polantz**, is seeking:

- Records of communication between former Attorney General Jeff Sessions and Deputy Attorney General Rod Rosenstein regarding the Special Counsel's Office and investigation, dating from May 2017, through November 2018
- *The officials that will be searched for this request are: Deputy Attorney General Rod Rosenstein*

The requester, **John Greenewald**, is seeking:

- Emails of Deputy Attorney General Rod Rosenstein, which were sent or received on March 24, 2019
- *The officials that will be searched for this request are: Deputy Attorney General Rod Rosenstein*

The requester, **Katelyn Polantz**, is seeking:

- Records of communication pertaining to Department recusal analysis and decisions pertaining to the Special Counsel's Office and Department officials

The requester, **Katelyn Polantz**, is seeking:

- Records of communication between Deputy Attorney General Rosenstein and Special Counsel Mueller or his office.
- *The officials that will be searched for this request are: Deputy Attorney General Rod Rosenstein*

The requester, **Katelyn Polantz**, is seeking:

- Record of requests Attorney General William Barr made to Special Counsel Robert Mueller his office pertaining to explanation of investigative or prosecutorial steps, dating from February 2019, through March 2019

The requester, **Paul Kamenar of the National Legal and Policy Center**, is seeking:

- Various records pertaining to the appointment of the Special Counsel (See Attached)

Thank you!

-Gabi



---

**From:** OIP-NoReply  
**Sent:** Tuesday, April 16, 2019 11:45 AM  
**To:** Leeman, Gabrielle (ODAG)  
**Cc:** Villanueva, Valeree A (OIP)  
**Subject:** Notification of Records Search to be Conducted in Response to the FOIA, Jason Leopold, OIP No. DOJ-2019- 003019  
**Attachments:** Initial Request (3.18.19).pdf

The purpose of this email is to notify you that the records of the below-listed officials will be searched in response to the attached Freedom of Information Act (FOIA) request.

**Should you have any questions concerning this matter, please feel free to reply to or call - Valeree Villanueva x44594**

---

The requester, Jason Leopold, is seeking:

- Records pertaining to discussions between former Federal Bureau of Investigation Acting Director McCabe and Deputy Attorney General Rosenstein (see attached request)
- Timeframe: February 1, 2017 - July 31, 2017

The officials that will be searched for this request are:

- Deputy Attorney General Rod Rosenstein
- Edward O'Callaghan
- Corey Ellis
- Antoinette Bacon
- Matthew Baughman
- Adam Braverman
- Steven Cook
- Tashina Gauhar
- Andrew Goldsmith
- Brendan Groves
- Patrick Hovakimian
- Stacie Harris
- Ted Hunt
- Iris Lan
- Mark Masling
- Mark Michalic
- John Moran
- Paul Perkins
- Andrew Peterson
- Sujit Raman

- Matthew Sheehan
- Robyn Thiemann
- Bradley Weinsheimer
- David Wetmore
- (b) (6)
- SeLena Powell
- Please advise our office if any of the above custodians should be included or removed from this search.

The FOIA requires agencies to conduct a reasonable search in response to FOIA requests. For your information, this search will encompass the email and computer files (e.g. C or H drive) maintained by the officials listed above.

**To the extent officials within your office maintain other types of records, such as paper records or material maintained within a classified system that would be responsive to this request, but would not be located as a result of OIP's unclassified electronic search, please indicate so in response to this email as soon as possible.** OIP staff will make arrangements to conduct those searches as necessary. Similarly, if your office would not maintain any records responsive to this request and/or you can readily identify the officials, be they either current or former employees, who would maintain records responsive to this request, you may indicate so in response to this email.

Please note that the Federal Records Act, as amended in 2014 and [DOJ Policy Statement 0801.04](#) provide that government employees should not use a non-official account including, but not limited to, email, text, or instant message, for official business. However, should this occur, the communication must be fully captured in a DOJ recordkeeping system – either by copying any such messages to one's official account or forwarding them to one's official account within twenty days. Should any records custodians have official records responsive to this FOIA request, which are maintained only in a non-official account, and not copied into an official account, then those records should be provided to OIP.

ATTACHMENT (Initial Request Ltr)

**Please do not reply to this e-mail, as this account is not monitored. Thank you.**

---

Initial Request Staff  
Office of Information Policy  
U.S. Department of Justice

202-514-3642 (Main Line)  
202-514-1009 (Fax)

## DOJ-2019-003019 request Details

Due Date: 04/15/2019 Clock Days: 5

## Requester Information

<b>Requester</b>	Mr. Jason Leopold	<b>Tracking Number</b>	DOJ-2019-003019
<b>Organization</b>	Investigative Reporter	<b>Submitted Date</b>	03/18/2019
<b>Requester Has Account</b>	Yes	<b>Received Date</b>	03/18/2019
<b>Email Address</b>	(b) (6)	<b>Perfected Date</b>	03/18/2019
<b>Phone Number</b>	(b) (6)	<b>Last Assigned Date</b>	03/18/2019
<b>Fax Number</b>		<b>Assigned To</b>	Steffon L Edmonds
<b>Address</b>	(b) (6)	<b>Last Assigned By</b>	(Department of Justice - Office of Information Policy) Valeree Villanueva
<b>City</b>			(Department of Justice - Office of Information Policy)
<b>State/Province</b>		<b>Request Track</b>	Complex
<b>Zip Code/Postal Code</b>		<b>Fee Limit</b>	\$25.00

## Request Handling

<b>Requester Info Available to the Public?</b>	No	<b>Request Type</b>	FOIA
<b>Request Track</b>	Complex	<b>Request Perfected</b>	Yes
<b>Fee Category</b>	N/A	<b>Perfected Date</b>	03/18/2019
<b>Fee Waiver Requested</b>	Yes	<b>Acknowledgement Sent Date</b>	
<b>Fee Waiver Status</b>	Pending	<b>Unusual Circumstances</b>	No
<b>Expedited Processing Requested</b>	No	<b>Litigation</b>	No
<b>Expedited Processing Status</b>		<b>Court Docket Number</b>	
		<b>5 Day Notifications?</b>	No

# Description

---

## Long Description

I request disclosure from the Department of Justice Office of the Attorney General, Office of the Deputy Attorney General any and all records mentioning or referring to discussions between then FBI Acting Director Andrew McCabe and Deputy Attorney General Rod Rosenstein in which the two officials referred to and/or discussed the 25th Amendment and Mr. Rosenstein secretly wearing a wire or recording device in the White House. The time frame for this request is February 1, 2017 through July 31, 2017. I also request disclosure of any and all records from the same offices as well as the Office of Public Affairs that mentions or refers to the New York Times report about these discussions. The New York Times report is dated September 21, 2018. I request disclosure of records that covers the timeframe September 14 through September 30, 2018. The New York Times report can be found here:

<https://www.nytimes.com/2018/09/21/us/politics/rod-rosenstein-wear-wire-25th-amendment.html> Reasonably Foreseeable Harm. The FOIA Improvement Act of 2016 amended the FOIA as follows (5 USC 552(a)(8)): (A) An agency shall— (i) withhold information under this section only if— (I) the agency reasonably foresees that disclosure would harm an interest protected by an exemption described in subsection (b); or (II) disclosure is prohibited by law; and (ii) (I) consider whether partial disclosure of information is possible whenever the agency determines that a full disclosure of a requested record is not possible; and (II) take reasonable steps necessary to segregate and release nonexempt information. . . . DOJ and its components should not fail to meet the requirements of Section 552(a)(8) when processing my request and release responsive records to me in full or at least in part.

## Has Description Been Modified?

No

## Description Available to the Public?

No

## Short Description

records of discussions between DAG and FBI's McCabe re: 25th amendment or wearing a wire.

# Additional Information

---

## Litigation Counsel Name

N/A

## Litigation Case Number

N/A

## Litigation Contact Information

N/A

## Sub-Office - IR

Office of Information Policy

## Clearwell Number

N/A

## Subject to Litigation?

N/A

## Processing Queue

N/A

## Acknowledged?

N/A

# Attached Supporting Files

---

# Assigned Tasks

---

Outcome	Task Type	Assigned To	Assigned By	Submitted Date	Due Date	Closed Date	Notification	Justification
Pending	Fee Waiver	DOJ	Mr. Jason Leopold	03/18/2019	03/18/2019		No	
Requester Justification	<p>I am the senior investigative reporter for BuzzFeed News and formerly senior investigative reporter and on-air correspondent for VICE News. Additionally, my reporting has been published in The Guardian, The Wall Street Journal, Financial Times, Salon, CBS Marketwatch, The Los Angeles Times, The Nation, Truthout, Al Jazeera English and Al Jazeera America.</p> <p>I request a complete waiver of all search and duplication fees. If my request for a waiver is denied, I request that I be considered a member of the news media for fee purposes.</p> <p>Under 5 U.S.C. §552(a)(4)(A)(iii), "Documents shall be furnished without any charge ... if disclosure of the information is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in the commercial interest of the requester." Disclosure in this case meets the statutory criteria, as the records sought detail the operations and activities of government. This request is also not primarily in the commercial interest of the requester, as I am seeking the records as a journalist to analyze and freely release to members of the public.</p> <p>If I am not granted a complete fee waiver, I request to be considered a member of the news media for fee purposes and willing to pay all reasonable duplication expenses incurred in processing this FOIA request.</p> <p>I will appeal any denial of my request for a waiver administratively and to the courts if necessary.</p>							

The following list contains the entire submission, and is formatted for ease of viewing and printing.

---

## Contact information

<b>First name</b>	Leslie
<b>Last name</b>	Gillispie
<b>Mailing Address</b>	(b) (6)
<b>City</b>	(b) (6)
<b>State/Province</b>	(b) (6)
<b>Postal Code</b>	(b) (6)
<b>Country</b>	United States
<b>Phone</b>	(b) (6)
<b>Email</b>	(b) (6)

---

## Request

<b>Request ID</b>	52621
<b>Confirmation ID</b>	52096
<b>Request description</b>	I would like all documents relating to the appointment of Robert Mueller to investigate Russia collusion and obstruction of justice. I want documents that support the appointment of the Special Counsel in 2016.

---

## Supporting documentation

---

### Fees

<b>Request category ID</b>	other
<b>Fee waiver</b>	no

---

## Expedited processing

<b>Expedited Processing</b>	no
-----------------------------	----



**FOIA COVER SHEET***Justice Management Division / Logistics Management Services**Mail Referral Unit, Landover Operations Center, RM 115***TO:**

Date	3/19/19
Components/POCs	OIP/Laurie Day

**REQUEST INFORMATION:**

FOIA Tracking Number	EMRUFOIA031519-4
Requester	Robert Arthur
Date of Request	3/15/19
Date Received	3/15/19
Processed By (initials):	KC

**REMARKS:**

The MRU has reviewed the attached FOIA request and is sending it to your office for processing. A letter was also sent to the requestor advising him of this referral. If you have any questions, please contact Joe Gerstell o (b) (6).

U.S. Department of Justice



---

Washington, D.C. 20530

March 19, 2019

Robert Arthur

(b) (6)

Dear Sir/Madam:

This is in response to your request for records, Tracking Number, EMRUFOIA031519-4. Your Freedom of Information Act and/or Privacy Act (FOIA/PA) request was received by this office which serves as the receipt and referral unit for FOIA/PA requests addressed to the Department of Justice (DOJ). Federal agencies are required to respond to a FOIA request within 20 business days. This period does not begin until the request is actually received by the component within the DOJ that maintains the records sought, or ten business days after the request is received in this office, whichever is earlier.

We have referred your request to the DOJ component(s) you have designated or, based on descriptive information you have provided, to the component(s) most likely to have the records. All future inquiries concerning the status of your request should be addressed to the office(s) listed below:

FOIA/PA  
Office of Information Policy  
Department of Justice  
Suite 11050  
1425 New York Avenue, N.W.  
Washington, DC 20530-0001  
(202) 514-FOIA

Sincerely,

MRUFOIA  
Logistics Management  
Facilities and Administrative Services Staff  
Justice Management Division

---

**From:** Rosenstein, Rod (ODAG)  
**Sent:** Tuesday, May 7, 2019 6:39 PM  
**To:** Sutton, Sarah E. (OPA)  
**Subject:** RE: Exit Interviews

OK. Please try to set u (b) (5) for tomorrow.

---

**From:** Sutton, Sarah E. (OPA) (b) (6) >  
**Sent:** Tuesday, May 7, 2019 6:27 PM  
**To:** Rosenstein, Rod (ODAG) (b) (6) >  
**Subject:** RE: Exit Interviews

Following up on this. I am attaching the email fro (b) (5) with their pitch to you. Happy to help with logistics you are interested.

Also, if you wanted to do an exit interview wit (b) (5). Happy to help coordinate that as well (b) (5). Should you want to do it, it would be on the record.

One last option would b (b) (5). If there's one you're interested in then I can help schedule it, or connect you with the right people if that's something you would like to do.

Thanks!

---

**From:** Sutton, Sarah E. (OPA)  
**Sent:** Monday, May 6, 2019 5:29 PM  
**To:** Rosenstein, Rod (ODAG) (b) (6) >  
**Subject:** Exit Interviews

The below names have reached out to you wanting an exit interview. Let me know if you are interested in doing any of these before you leave! If so, I'm happy to help coordinate. Should you want to do these after you leave the Department, I can get all the contact info you would need as well.

(b) (5)

- (b) (5)

(b) (5)

- (b) (5)

(b) (5)

- (b) (5)

(b) (5)

(b) (5)

(b) (5)

Thanks!

**Sarah Sutton**  
Department of Justice  
Office of Public Affairs

(b) (6)

# Chat with Edward C. O'Callaghan

4/18/2019 9:28:46 AM - 5/10/2019 6:26:02 AM

---

## Export Details:

Device Phone Numb (b) (6)

Device Name Rod Rosenstein iPhone

Device ID (b) (6)

Backup Date Wednesday, May 22, 2019 12:29 PM

Backup Directory C:\Users\cgreer\AppData\Roaming\Apple Computer\MobileSync\Backu (b) (6)

iOS 11.2.6

Current Time Zone (UTC-05:00) Eastern Time (US & Canada)

Created with iExplorer v4.2.6.0

## Participants:

(b) (6), Edward C. O'Callaghan

---

Thursday, April 18, 2019

(b)(6) Edward O'Callaghan

Ag headed up

9:28 AM

Friday, April 19, 2019

(b)(6) Rod Rosenstein

<https://www.usatoday.com/story/news/politics/2019/04/19/ag-barr-center-political-firestorm-after-mueller-report-release/3519319002/>

6:22 PM

Sunday, April 21, 2019

(b)(6) Edward O'Callaghan

He's done everything he should do, and nothing that he shouldn't," said former Attorney General Michael Mukasey, who served under President George W. Bush. "The bottom line is that nothing got obstructed."

Mukasey also said that Barr was justified to make the final determination that Trump's conduct did not rise to obstruction.

2:22 PM

"Hell, yes!" Mukasey said, endorsing Barr's intervention. "Somebody had to make the decision."

Monday, April 22, 2019

(b)(6) Edward O'Callaghan

I need to go back to apt to get my laptop so I will just meet you in office. Thanks.

9:24 AM

Tuesday, April 23, 2019

(b)(6) Rod Rosenstein

I will be there in a few minutes

9:00 AM

(b)(6) Edward O'Callaghan

Ok. Ag moved our meeting to 9:30 today

9:00 AM

(b)(6) Edward O'Callaghan



Sorry 9:15.

9:00 AM

Wednesday, April 24, 2019

(b)(6) Edward O'Callaghan

Do you have your binder and materials for the 1:00 meeting? Just checking. I can bring over with me if not.

11:51 AM

(b)(6) Rod Rosenstein

Yes I do.

11:54 AM

(b)(6) Edward O'Callaghan

Ok

11:54 AM

(b)(6) Edward O'Callaghan



You can't leave until someone wins!!

10:19 PM

(b)(6) Edward O'Callaghan

U still there?

11:29 PM

Thursday, April 25, 2019

(b)(6) Rod Rosenstein

Until the bitter end

12:07 AM

(b)(6) Rod Rosenstein

<https://twitter.com/MaxBoot/status/1121043181053702144>

12:36 AM

(b)(6) Edward O'Callaghan

<https://apple.news/A76TGMxHRTKqjTs1ngXyuYg>

8:18 AM

(b)(6) Edward O'Callaghan

Spoke to Zach yesterday. Happy to discuss when you are free.

9:04 AM

(b)(6) Edward O'Callaghan

Just saw your sister on Fox!

6:22 PM

(b)(6) Edward O'Callaghan



Discussing measles outbreaks

6:25 PM

(b)(6) Edward O'Callaghan

FYI I asked for time with AG tomorrow to discuss the possible gtmo project. Any reason not to post your discussion with Jeff yesterday?

9:11 PM

(b)(6) Rod Rosenstein

Let's discuss.

9:12 PM

(b)(6) Edward O'Callaghan

Ok

9:13 PM



Saturday, April 27, 2019

(b)(6) Rod Rosenstein

...not. Federal prosecutors work with grand juries to assess evidence to determine whether a crime has been committed. Once a prosecutor has adequately investigated the facts of a case, he faces a binary choice: either to commence or to decline prosecution. To commence prosecution, the prosecutor must conclude both that the subject's conduct constitutes a federal offense and that the admissible evidence is sufficient to obtain and sustain a guilty verdict by an unbiased trier of fact. These principles govern the conduct of all prosecutions by the Department of Justice and are codified in the Justice Manual.

The appointment of a Special Counsel and the targeting of the President of the United States as an investigative subject do not change these rules. To the contrary, they make it all the more important for the Department to follow them. The appointment of a Special Counsel calls for particular care it poses the risk of what Attorney General Robert Jackson called "the most dangerous power of the prosecutor: that he will pick people that he thinks he should get, rather than pick cases that need to be prosecuted." By definition, a Special Counsel is charged to consider prosecution of particular subjects, not to find the most meritorious cases to prosecute wherever they may be found. While this deviation from ordinary procedure is sometimes necessary, it also requires an extra measure of circumspection. Including a democratically elected politician as a target in a criminal investigation likewise calls for special care. And the President of the United States is a paradigmatic case. As Jackson admonished his United States Attorneys, politically sensitive cases demand that federal prosecutors be "dispassionate and courageous" in order to "protect the spirit as well as the letter of our civil liberties."

The core civil liberty in our American criminal justice system is the presumption of innocence. Every person enjoys this presumption long before the commencement of any investigation or official proceeding. A federal prosecutor's task is to decide whether the evidence is sufficient to overcome that presumption. If so, she seeks an indictment; if not, she does not. The Special Counsel's report demonstrates that there are many subsidiary considerations informing that prosecutorial judgment—including whether particular legal theories would extend to the facts of the case and whether the evidence is sufficient to

9:45 AM

(b)(6) Edward O'Callaghan

I have a few edits/suggestions I will send around.

10:00 AM

Tuesday, April 30, 2019

(b)(6) Edward O'Callaghan

Thoughts are tha (b) (5)

7:46 PM

(b)(6) Rod Rosenstein

Success in these jobs is measured by degree.

7:55 PM

Thursday, May 2, 2019

(b)(6) Edward O'Callaghan



9 is pushed to 9:30

9:01 AM

Tuesday, May 7, 2019

(b)(6) Edward O'Callaghan

Please call when convenient

8:21 AM

(b)(6) Edward O'Callaghan

(b)(6) Edward O'Callaghan

8:28 AM

(b)(6) Rod Rosenstein

I left a message

8:41 AM

(b)(6) Edward O'Callaghan

<https://www.reuters.com/article/us-usa-immigration-asylum-exclusive-idUSKCN1SA0LG>

4:54 PM

Friday, May 10, 2019

(b)(6) Edward O'Callaghan

Ag moved morning meeting up to 8:55 so he can make speaking engagement

6:26 AM