U.S. Department of Justice
Office of the Deputy Attorney General

The Deputy Attorney General

Washington, D.C. 20530

June 3, 2021

MEMORANDUM FOR ALL FEDERAL PROSECUTORS

FROM: THE DEPUTY ATTORNEY GENERAL

SUBJECT: Guidance Regarding Investigations and Cases Related to Ransomware and Digital Extortion

Recent ransomware attacks—including the attack last month on Colonial Pipeline—underscore the growing threat that ransomware and digital extortion pose to the Nation, and the destructive and devastating consequences ransomware attacks can have on critical infrastructure.

A central goal of the recently launched Ransomware and Digital Extortion Task Force is to ensure that we bring to bear the full authorities and resources of the Department in confronting the many dimensions and root causes of this threat. We know that ransomware attacks and digital extortion schemes are often conducted by transnational criminal actors, spread without regard to geographic borders, and thrive on the abuse of online digital and financial infrastructure. Accordingly, the Department must make sure that its efforts in combating digital extortion are focused, coordinated, and appropriately resourced. To ensure we can make necessary connections across national and global cases and investigations, and to allow us to develop a comprehensive picture of the national and economic security threats we face, we must enhance and centralize our internal tracking of investigations and prosecutions of ransomware groups and the infrastructure and networks that allow these threats to persist.

The United States Attorneys' Offices, the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS) and Money Laundering and Asset Recovery Section (MLARS), the National Security Division (NSD), and the Federal Bureau of Investigation (FBI), among other components across the Justice Department, play a critical role in identifying those who engage in these schemes and in developing lawful options to disrupt and dismantle the infrastructure and networks used to carry out these attacks. To ensure a coordinated Department-wide approach, this Memorandum highlights certain existing Justice Manual requirements, and sets forth new requirements relating to ransomware or digital extortion attacks and investigations and cases with a nexus to ransomware and digital extortion. These new requirements are effective immediately.

Scope of this Policy

The requirements in this memorandum apply to all investigations and cases that involve:

a. ransomware and/or digital extortion; or

b. a subject or target under investigation primarily for the unlawful operation of infrastructure frequently used in ransomware and digital extortion schemes, including but not limited to:

i. Counter anti-virus services;

ii. Illicit online forums or marketplaces that advertise or sell ransomware, digital extortion, or hacking tools and network access credentials (i.e., vectors by which ransomware may infect a network, including Remote Desktop Protocol credentials or shells);

iii. Cryptocurrency (or digital currency) exchanges, mixers, or tethers;

iv. Bulletproof hosting services;

v. Botnets; and

vi. Online money laundering services.

Notification and Urgent Reports Related to Ransomware or Digital Extortion Cases, Investigations, or Attacks

1) **Notifications in Investigations and Cases:** An assigned Assistant United States Attorney (AUSA) (or a U.S. Attorney's Office's Computer Hacking and Intellectual Property (CHIP) Coordinator) or Trial Attorney must notify CCIPS and the National Security & Cyber Crime Coordinator for the Executive Office for United States Attorneys (EOUSA) of the opening of, or any significant new development in, an investigation or case falling within the scope of this memorandum. Significant new developments include new charges, pleas, dismissals, trial dates, and sentencings. In addition, in any instance in which a United States Attorney's Office learns of a ransomware or digital extortion attack in its District, regardless of whether it implicates an open matter or case, the United States Attorney's Office shall, as soon as practicable, notify CCIPS and the National Security & Cyber Crime Coordinator for EOUSA.

2) **Urgent Reports:** Consistent with obligations in the Justice Manual, an Urgent Report should be filed in **every** instance in which a United States Attorney's Office learns of either a new ransomware or digital extortion attack in its District, or an attack believed to be related to an ongoing ransomware or digital extortion investigation or case it is conducting, that constitutes (a) a major development in the case; (b) a law enforcement emergency; or (c) an event affecting the Department that is likely to generate national media or Congressional attention. *See* JM 1-13.100. Urgent Reports should be

submitted, for instance, when a United States Attorney's Office learns of a ransomware attack on critical infrastructure or upon a municipal government in their District.

3) **Means of Notification:** All notifications required under this policy must be made as soon as practicable by email to USAEO.Ransomware-Case@usdoj.gov. Urgent Reports should also be separately submitted, when required, through normal means. *See* JM 1-13.140. CCIPS and EOUSA will consult with the prosecuting office if more detailed notifications are needed.

Coordination with CCIPS

1) CCIPS, consistent with its duties under Justice Manual 9-50.400, Coordination and Notification, shall be responsible for cases across the Department that fall within the scope of this policy. CCIPS will be assisted by EOUSA in its efforts to track and monitor ongoing developments in ransomware and digital extortion attacks, investigations, and cases, as set forth above. Where CCIPS becomes aware that an investigation relates to another active investigation, CCIPS shall notify all relevant offices to ensure proper coordination. CCIPS will coordinate with other Department components, including MLARS and the National Security Division, Counterintelligence and Export Control Section (CES), as appropriate regarding any ransomware and digital extortion-related matter that implicates criminal prosecutions subject to their respective approvals or authorizations.

2) When CCIPS becomes aware of an investigation or case that falls within the scope of this policy but where the assigned prosecutor has not yet notified EOUSA, CCIPS shall notify the relevant office(s) and EOUSA, and the investigation or case shall be subject to the requirements of this policy going forward.

3) All United States Attorneys' Offices and litigating divisions are reminded of their obligation to consult with CCIPS with respect to decisions to charge a case under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, including through the use of the CFAA Consultation Request form on CCIPS Online, *available at* https://dojnet.doj.gov/criminal/ccips/forms/cfaa-consultation-request.php. *See* JM 9-50.400.

4) To ensure accuracy and consistency in this high-priority area, public statements about any cases falling within the scope of this memorandum shall be coordinated among the prosecuting office(s), CCIPS, other relevant components, and the Department's Office of Public Affairs (OPA).

Existing Justice Manual Provisions Unaffected

Any investigation or case falling within the scope of this policy remains subject to any applicable existing Justice Manual provisions and requirements, including reporting requirements to or approvals from the Criminal Division and the National Security Division, as required.

Updates to the Justice Manual

The Justice Manual will be updated to reflect the new requirements outlined herein.