FOR IMMEDIATE RELEASE
September 17, 2024

DOJ OIG Releases Report on DOJ's Strategy to Combat and Respond to Ransomware Threats and Attacks

Department of Justice (DOJ) Inspector General Michael E. Horowitz announced today the release of a report assessing the DOJ's strategy to combat ransomware threats, including its coordination and response to ransomware attacks. Ransomware, a form of malicious software that encrypts files on a victim's device which renders them unusable, has become a lucrative crime and a costly and destructive threat to business and government. Due to the evolving techniques employed by ransomware actors, which has led to an increase in the scale, scope, and frequency of attacks, combatting the ransomware threat is a formidable task.

The DOJ Office of the Inspector General (OIG) found that the Federal Bureau of Investigation (FBI) and the DOJ Criminal Division's Computer Crime and Intellectual Property Section have led the DOJ's response and prioritized their efforts to maximize ransomware attack prevention. In addition, the FBI developed a ransomware strategy focused on targeting the ransomware ecosystem, which enabled significant disruptions of three ransomware groups in 2023.

The OIG's findings also included the following opportunities for improvement:

- **DOJ's Existing Metrics for Ransomware do not Capture the Effectiveness of Its Disruptive Activities Against Malicious Actors.** DOJ established combatting ransomware attacks as a DOJ Agency Priority Goal for fiscal years 2022 and 2023. However, the existing metrics do not capture the effectiveness of its disruptive activities against malicious actors because they did not account for DOJ's shift from arrests and indictments, which are challenging in ransomware cases, towards DOJ actions to disrupt both ransomware actors and the broader cybercriminal ecosystem.

- **DOJ's Deconfliction Policy for Cyber Threats has not Been Implemented Consistently**. United States Attorney's Offices differed in their awareness and implementation of the DOJ's deconfliction policy for cyber threats, leading to deconfliction challenges on ransomware investigations. Failing to coordinate and deconflict can result in damage to investigations, prosecutions, and relationships with domestic and international partners and victims, as well as wasted resources, all of which can undermine public safety, national security, and confidence in DOJ.

- **The FBI Should Better Define the FBI's National Cyber Investigative Joint Task Force Criminal Mission Center's Ransomware Role to Ensure its Contributions are Meaningful and Effective**. The FBI's National Cyber Investigative Joint Task Force Criminal Mission Center was responsible for coordinating whole-of-government ransomware plans in 2021 and 2022. However, in 2022 Congress established a new, multi-agency Joint Ransomware Task Force to coordinate whole-of-government responses to ransomware threats. We found that the creation of the Joint Ransomware

Task Force impacted the role of the Criminal Mission Center, leaving its ransomware role not well defined.

The DOJ OIG made three recommendations to improve DOJ's management of the ransomware threat. DOJ, through the FBI and Office of the Deputy Attorney General, agreed with all three recommendations.

Report: Today's report can be found on the OIG's website.

###