Audit of the Department of Justice's Strategy to Combat and Respond to Ransomware Threats and Attacks

★ ★ ★

AUDIT DIVISION

24-107

SEPTEMBER 2024

EXECUTIVE SUMMARY

Audit of the Department of Justice's Strategy to Combat and Respond to Ransomware Threats and Attacks

Objective

To assess the Department of Justice's (DOJ or Department) strategy to combat ransomware threats, including its coordination and response to ransomware attacks. This audit focused on the Department's general approach to combatting ransomware attacks and not its activities for combatting attacks on the Department itself.

Results in Brief

Ransomware is a form of malicious software that encrypts files on a victim's device, rendering them unusable. Malicious actors then demand ransom payments to restore the victim's access to the files. We found that the Federal Bureau of Investigation (FBI) and the DOJ Criminal Division's Computer Crime and Intellectual Property Section (CCIPS), which lead the Department's ransomware efforts, have prioritized the ransomware threat and allocated existing resources in an effort to maximize their impact. The FBI also co-leads the multi-agency Joint Ransomware Task Force (JRTF), established by Congress in 2022, to coordinate federal efforts for the ransomware threat.

We also identified opportunities for the Department to improve its efforts to combat the ransomware threat. Specifically, we found the Department lacked impactful metrics for measuring success against ransomware and that it could improve compliance with its deconfliction policy for ransomware. We also found that the FBI-led National Cyber Investigative Joint Task Force (NCIJTF) Criminal Mission Center, which was responsible for coordinating whole-of-government ransomware plans in 2021 and 2022, did not produce meaningful outcomes in combatting ransomware and that its role in this area has been undefined since Congress created the JRTF in 2022.

Recommendations

Our report contains a total of three recommendations for the Office of the Deputy Attorney General (ODAG) and the FBI to improve the Department's efforts to combat ransomware.

Audit Results

Ransomware attacks have increased in scale, scope, and frequency over the past decade. There are different types of ransomware, each of which is referred to as a "variant." These variants can differ in their delivery mechanisms, target selection, technical proficiency, method of extortion, and numerous other factors. Variants often change and new ones frequently emerge, further complicating efforts to effectively combat this threat.

The FBI and CCIPS Led the DOJ's Efforts to Prioritize and Respond to the Ransomware Threat

We found that the FBI and CCIPS have prioritized the ransomware threat and allocated existing resources to maximize their impact. The FBI has developed a framework to prioritize and assess a ransomware variant's impact on a recurring basis. The results of these assessments are used by the FBI to identify intelligence production needs for its high-priority investigations and by CCIPS to determine the level of support needed to maintain coverage of cases involving significant variants. Further, the FBI developed a ransomware strategy focused on targeting the actors, infrastructure, and finances that comprise and enable the ransomware ecosystem.

The DOJ Should Improve its Metrics to Track Progress and Impact for the Ransomware Threat

The Department announced that combatting ransomware attacks was a DOJ Agency Priority Goal for the period covering fiscal years (FY) 2022 and 2023 to: (1) increase the percentage of reported ransomware incidents where cases are opened, added to existing cases, resolved or action was taken within 72 hours to 65 percent; and (2) increasing the number of seizures or forfeitures in ransomware matters by 10 percent. However, DOJ had not published its action plan or reported any progress for this goal for FYs 2022 or 2023 on performance.gov, as required.

The Department has not yet announced its goals for the next 2-year period covering FYs 2024-2025. However, we believe the Department's existing metrics for ransomware do not capture the effectiveness of its disruptive activities against malicious actors. Regardless of whether the Department maintains ransomware as a priority goal, it should determine which metrics are most impactful to ensure they capture the effectiveness of its actions to combat the ransomware threat.

The ODAG Should Assess its Deconfliction Policy to Ensure Consistent Implementation and Compliance

According to the ODAG, failure to coordinate and deconflict can damage investigations, prosecutions, and relationships that are critical to law enforcement; waste resources; and undermine public safety, national security, and confidence in the Department. To address these concerns, in early 2023 the ODAG issued a policy to improve deconfliction and coordination of cyber investigations. The policy required prosecutors confirm that federal investigators conducted deconfliction throughout their investigations.

However, Department employees told us that there are continued issues with deconfliction of ransomware cases. For example, FBI officials cited an instance where federal prosecutors overseeing two related ransomware cases did not share information as the deconfliction policy intended, and a Criminal Division Official told us United States Attorney's Offices differed as to their awareness and implementation of the policy. In light of these anecdotal concerns, we recommend that the ODAG assess the implementation of its deconfliction policy in ransomware cases to ensure consistent implementation and compliance.

The FBI Should Better Define the NCIJTF Criminal Mission Center's Ransomware Role to Ensure its Contributions are Meaningful and Effective

The NCIJTF is led by the FBI and consists of three mission centers. Specifically, we assessed the NCIJTF Criminal Mission Center efforts for ransomware, including coordinating whole-of-government ransomware plans in 2021 and 2022, which did not result in meaningful outcomes. While the Criminal Mission Center coordinated plans for two ransomware variants, we found it could not demonstrate that the plan's strategic objectives and outcomes were met and did not produce final reports detailing lessons learned. FBI officials and stakeholders also expressed concerns about the Criminal Mission Center's information sharing and communication, lack of impactful support, and questioned its sense of urgency and adaptability amid a rapidly evolving threat environment. Ultimately, NCIJTF and FBI officials confirmed to us that they could not identify any disruptive action that originated from the Criminal Mission Center's ransomware efforts.

Further, Congress required the establishment of the multi-agency JRTF, in 2022, to coordinate whole-of-government responses to ransomware threats. We found that the creation of the JRTF impacted the role of the Criminal Mission Center, leaving this role not well defined. The FBI, as the responsible body for the NCIJTF, should better define the NCIJTF Criminal Mission Center's role for ransomware to ensure its contributions are meaningful and effective.

Table of Contents

Introduction

Ransomware is a form of malicious software designed to encrypt files on a victim's device and render data and systems unusable. Malicious actors then demand ransom payments in exchange for a decryption key to restore access to the locked data and systems. To intensify the threat and further incentivize payment, ransomware actors also threaten to publish stolen data or sell it on the dark web. Ransomware has become a lucrative crime and a costly and destructive threat to business and government. In its Comprehensive Cyber Review from July 2022, the Department of Justice (DOJ or Department) stated that it has been countering the ransomware threat for over 8 years, dating back to at least the 2014 takedown of the GameOver Zeus botnet which was used to launch Cryptolocker ransomware attacks. Since 2014, the nature of the techniques employed by ransomware actors has evolved and led to an increase in the scale, scope, and frequency of attacks. There are different types of ransomware, each of which is referred to as a "variant." These variants can differ in their delivery mechanisms, target selection, technical proficiency, method of extortion, and numerous other factors. Variants often change and new ones frequently emerge, further complicating efforts to combat the threat.

FBI Ransomware Reporting from 2019 through 2023

- The Internet Crime Complaint Center received over 13,000 victim reports of ransomware attacks
- Over $181 million in reported victim losses
- Over 2,600 reports to IC3 per year, on average

While it is difficult to quantify the total number of ransomware attacks due to the voluntary nature of reporting and potential reluctance by victims to report attacks, in 2023, the FBI's Internet Crime Complaint Center (IC3) reported ransomware incidents were on the rise again (after a brief downturn in 2022), with over 2,825 complaints. This represents an increase of 18 percent from 2022. Reported losses rose 74 percent, from $34.3 million in 2022 to $59.6 million in 2023.[1] On July 19, 2022, the Deputy Attorney General emphasized that collaboration with the private sector is critical to disrupting malicious cyber activity, preventing future attacks, and holding cybercriminals accountable.[2] She further emphasized the importance of prompt reporting by victims of cyber attacks, especially those in the private sector.

---

[1] According to the FBI, reported losses does not include estimates of lost business, time, wages, files, or equipment, or any third-party remediation services acquired by an entity. In some cases, entities do not report any loss amount to the FBI, thereby creating an artificially low overall ransomware loss rate. Lastly, the number only represents what entities report to the FBI via the IC3 and does not account for the entity direct reporting to FBI field offices/agents.

[2] Deputy Attorney General Lisa O. Monaco, Keynote Address at International Conference on Cyber Security 2022, July 19, 2022. https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-delivers-keynote-address-international-conference

In the *Audit of the Federal Bureau of Investigation's Implementation of its Next Generation Cyber Initiative*, *15-29* (July 2015) the Office of the Inspector General (OIG) found that the FBI was working to develop strategies to enhance outreach to private sector entities because the private sector was reluctant to share information with the government due to concerns regarding balancing national security and individual privacy interests. In the *Audit of the Federal Bureau of Investigation's Cyber Victim Notification Process*, 19-23 (March 2019), the OIG reviewed the FBI's processes and practices for notifying and engaging with victims of cyber intrusions, including the importance of the FBI's relationship with the private sector.

As the Department has recognized for years, combatting the ransomware threat is a formidable task facing both government and private sector cybersecurity professionals, especially since most ransomware actors are based in countries that are unwilling or unable to prosecute this cybercrime. In June 2021, after a significant ransomware attack on critical infrastructure, the Deputy Attorney General stated, "There is no higher priority at the Department than using all available tools to protect our nation, including from ransomware and other digital threats."[3] On March 29, 2022, the FBI's Cyber Division Assistant Director testified that the ransomware threat has been one of the FBI's top cybercriminal investigative priorities and that multiple field offices respond to ransomware attacks daily. He noted the number of ransomware variants has grown and the FBI is investigating over 100 variants, many of which have been used in multiple ransomware attacks.[4] And in recent years, the emergence of the ransomware-as-a-service model, where a developer sells or leases ransomware tools to criminal customers, has lowered both the barrier to entry and level of technological savvy needed to carry out and profit from these attacks, resulting in more actors conducting ransomware attacks.

To demonstrate its commitment to combatting ransomware attacks and signal its prioritization of the ransomware threat, in April 2021 the Department established the Ransomware and Digital Extortion Task Force (Ransomware Task Force), which included several Department components. In so doing, the Department emphasized that the coordination of ransomware efforts was necessary to ensure that the whole of the U.S. government's resources would be brought to bear to address this threat in a systematic and comprehensive way, and that the task force would serve to focus and coordinate DOJ efforts and position the Department to effectively address this threat.[5]

The Office of the Deputy Attorney General (ODAG) memorandum that established the Ransomware Task Force also contained several strategic areas, including directing the Ransomware Task Force to design and implement a strategy to disrupt and dismantle the ransomware criminal ecosystem, specifying this strategy should include the use of all available criminal, civil, and administrative actions, such as the takedown of servers and seizures of ransomware proceeds. However, according to the ODAG, the Ransomware Task Force convened only two meetings, did not meet regularly to ensure the implementation of its strategic areas, and did not retain records of decisions or directions resulting from these meetings.[6] Instead, the FBI and Criminal Division's Computer Crime and Intellectual Property Section (CCIPS) led the Department's

---

[3] The Deputy Attorney General Delivers Remarks at a Press Conference on a Ransomware Attack on Critical Infrastructure, June 7, 2021. https://www.justice.gov/opa/speech/dag-monaco-delivers-remarks-press-conference-darkside-attack-colonial-pipeline

[4] Statement of Bryan A. Vorndran, Assistant Director of the FBI's Cyber Division, before the Committee on the Judiciary, U.S. House of Representatives, for a hearing entitled "Oversight of the FBI Cyber Division," March 29, 2022. https://docs.house.gov/meetings/JU/JU00/20220329/114533/HHRG-117-JU00-Wstate-VorndranB-20220329.pdf

[5] The Department also stated that the National Cyber Investigative Joint Task Force (NCIJTF) would help inform the Ransomware Task Force's efforts for this threat. The NCIJTF was established in January 2008 and created to serve as a focal point for coordinating and sharing pertinent information related to cyber threat investigations.

[6] While the Ransomware Task Force was not formally disbanded, its absence of meetings indicates that it is now defunct for all intents and purposes.

efforts, as detailed later in this report in the section titled "The FBI and CCIPS Led the DOJ's Efforts to Prioritize and Respond to the Ransomware Threat."

Currently, the Department's counter-ransomware efforts involve representation from across the Department, including:

Criminal Division

CCIPS is responsible for implementing the Department's national strategies in combatting computer and intellectual property crimes worldwide by working with other government agencies, the private sector, academic institutions, and foreign counterparts. Working in support of and alongside the U.S. Attorneys' Offices (USAO), CCIPS prosecutes violations of federal law involving cyber intrusions and attacks.

National Security Division

Among the highest priorities of the National Security Division's (NSD) Counterintelligence and Export Control Section are the investigation, disruption, and deterrence of national security cyber threats. Within the Counterintelligence and Export Control Section is a group of attorneys who partner with the FBI's Cyber Division and USAOs across the U.S. to investigate, disrupt, and deter malicious cyber activity by nation-state actors or their proxies, or other malicious cyber activity that jeopardizes national security. In June 2023, the National Security Cyber Section (NatSec Cyber) was created, in part to increase the scale and speed of disruption campaigns and prosecutions.

Executive Office for U.S. Attorneys

USAOs around the country have experience developing and prosecuting cyber cases and have established strong working relationships with the federal law enforcement agencies working in their districts. Additionally, the USAOs and CCIPS jointly established a network of criminal cyber experts more than 17 years ago, known as the Computer Hacking and Intellectual Property (CHIP) coordination network. CHIP prosecutors receive training and resources that help ensure they are prepared for the newest threats and are familiar with the latest technological trends being exploited by criminals, and this network also aids in the coordination of multi-district prosecutions involving cyber threats. In 2012, the National Security Cyber Specialist network was established and is focused on combatting cyber-based terrorism and state sponsored computer intrusions.

Federal Bureau of Investigation

The FBI's Cyber Division oversees field office efforts to investigate cyber threats, whether they stem from criminal or national security actors. Each of the FBI's 56 field offices across the country has a cyber squad that responds to and investigates ransomware attacks. As of February 2023, the FBI had 104 active ransomware investigations. The FBI also has roles with two multi-agency task forces with ransomware responsibilities:

- **The National Cyber Investigative Joint Task Force (NCIJTF)** is a multi-agency national focal point established in 2008 by presidential directive for coordinating, integrating, and sharing pertinent information related to cyber threat investigations. The FBI is responsible for operating the NCIJTF, however the authority does not grant the NCIJTF a role in directing the operations of other agencies. The NCIJTF's Criminal Mission Center coordinated whole-of-government ransomware campaigns before the creation of the Joint Ransomware Task Force.
- **The Joint Ransomware Task Force (JRTF)** was created in September 2022, pursuant to the Cyber Incident Reporting for Critical Infrastructure Act of 2022. The Department of Homeland

Security's Cybersecurity and Infrastructure Security Agency and the FBI co-lead the JRTF. The JRTF is a multi-agency task force focused on coordinating federal efforts to address the ransomware threat. JRTF's structure includes an Executive Steering Group, Strategic Coordination Group, and various working groups focused on different aspects of the ransomware threat.

Prior Reports

The U.S. Government Accountability Office (GAO) issued a report in September 2022 on federal efforts on ransomware.[7] The GAO report focused on federal efforts by eight agencies, including the FBI, to provide ransomware prevention and response assistance to state, local, tribal, and territorial government organizations. GAO reported that while state, local, tribal, and territorial government organizations were generally satisfied with federal ransomware assistance, there was room for improvement and that shortfalls existed, in part, because of a lack of an established mechanism for interagency collaboration. GAO recommended the Department (particularly the FBI) evaluate how best to address concerns and improve interagency coordination related to state, local, tribal, and territorial government organizations, while also facilitating collaboration with other key ransomware stakeholders. The Department and the FBI concurred with the recommendation and noted the formation of a working group that is part of the JRTF that includes the DOJ and various external partners. The FBI noted that the JRTF working group was created to collaborate with private sector entities and state, local, tribal, and territorial government law enforcement components on ransomware incidents. The working group is also responsible for facilitating the sharing of ransomware information, including tactics, tools, procedures, and indicators of compromise, as applicable. As of March 2024, the GAO recommendation to the Department and FBI was "Open - Partially Addressed."

Office of the Inspector General Audit Approach

The objective of this audit was to assess the Department's strategy to combat ransomware threats, including its coordination and response to ransomware attacks. Our audit generally covered, but was not limited to, counter-ransomware activities by the Department and the FBI from April 2021 through September 2023. We focused on the Department's general approach to combatting ransomware attacks and did not review the Department's specific approach or efforts related to combatting attacks on the Department itself. While ransomware is primarily a cybercriminal threat, when a ransomware attack disrupts or threatens the operations of a significant critical infrastructure organization or involves state sponsored activity, there are national security ramifications. Our audit focused on the cybercriminal piece of the ransomware threat. To accomplish our objective, we:

- Interviewed Department officials and analyzed information from the ODAG, FBI, NCIJTF; Justice Management Division, Criminal Division, NSD, Executive Office for U.S. Attorneys, and a USAO;

- Assessed the Department's support of the Ransomware Task Force and efforts to measure progress against the ransomware threat through its Agency Priority Goal;

[7] GAO, *Federal Agencies Provide Useful Assistance but Can Improve Collaboration*, GAO-22-104767 (September 2022), https://www.gao.gov/products/gao-22-104767 (accessed March 2024).

- Reviewed NCIJTF counter-ransomware efforts, including guidance developed to support U.S. counter-ransomware activities and plans developed for specific ransomware variants;

- Reviewed FBI Cyber Division efforts to prioritize the ransomware threat, including development of a strategy, unit restructuring, case classification enhancement, and building awareness of resources, tools, and techniques to combat the threat.

Appendix 1 contains further details on our audit objective, scope, and methodology.

Audit Results

We assessed the DOJ's efforts to address the ransomware threat and found the FBI and CCIPS led the DOJ's response and prioritized their efforts to maximize impact. In addition, the FBI developed a ransomware strategy focused on targeting the ransomware ecosystem, which enabled significant disruptions of three ransomware groups in 2023. Additionally, we assessed the Department's Agency Priority Goal for ransomware and its deconfliction guidance for cyber investigations. We found the Department's metrics for ransomware did not account for DOJ efforts to disrupt ransomware actors and its ecosystem and that the Department should assess its deconfliction guidance for cyber investigations to ensure consistent implementation and compliance by prosecutors for ransomware cases.

Lastly, we assessed the National Cyber Investigative Joint Task Force (NCIJTF) Criminal Mission Center's efforts to coordinate whole-of-government plans for ransomware in 2021 and 2022. While the Criminal Mission Center coordinated plans for two ransomware variants, we found neither resulted in meaningful outcomes and it stopped holding its ransomware operational planning meetings in September 2022, around the same time the JRTF was formally established. We also found the Criminal Mission Center's role for ransomware has evolved after the JRTF was created and the FBI should better define its role to ensure its support of the JRTF and contributions for ransomware are meaningful and effective.

The FBI and CCIPS Led the DOJ's Efforts to Prioritize and Respond to the Ransomware Threat

We found that the FBI and CCIPS, which works alongside the USAOs to prosecute violations of federal law involving cyber intrusions and attacks, were the primary components driving the Department's efforts in response to the ransomware threat. Both components prioritized the evolving ransomware threat, including identifying how to allocate existing resources for the most impact.

Both CCIPS and the FBI have employed the concept of using criminal legal authorities to disrupt or take down online criminal infrastructure, such as botnets, which has led to several significant successes. For instance, in January 2021 the FBI and CCIPS led an effort to disable the Emotet botnet responsible for the mass distribution of ransomware and, in a separate action that same month, disrupted the NetWalker ransomware variant. In August 2023, the Department announced the disruption of the Qakbot botnet and malware responsible for millions of dollars in damage worldwide. In 2023, CCIPS had 108 open ransomware cases. A CCIPS official stated its strategy has been to apply resources to the ransomware cases where they can provide the most impact. For example, when the Department and the FBI worked to disrupt a high-profile ransomware group in late 2023, CCIPS assigned additional attorneys to provide extra support, in part because the USAO working the case was a small office with limited resources.

At the FBI, the Cyber Division made changes to better align its Cyber Criminal Operations Section with its ransomware threat prioritization, which resulted in the creation of a second Major Cyber Crimes Unit, focused solely on ransomware and malware to better respond to the ransomware threat. In addition, the FBI created a framework to prioritize and assess ransomware variants that are most impactful to U.S. interests. The FBI conducts the assessments every 6 months and shares the results within the Department

and, when necessary, with external U.S. government partners. For example, the FBI identified the Sodinokibi, Conti, and LockBit variants as high priority variants, which aligned with ongoing efforts to support those investigations, including targeting support, such as intelligence analysis about threat actors, and staff augmentation from FBI headquarters. A CCIPS official said CCIPS uses the results of FBI's ransomware assessment to determine the level of CCIPS support needed on particular ransomware cases and to ensure it maintains coverage over cases involving the most significant ransomware variants.

The FBI's Ransomware Strategic Pillars

Identify and Understand

Develop a thorough understanding of the criminal ecosystem through an integrated and collaborative intelligence effort with U.S. Government, partners, and allies.

Prioritize and Target

Prioritize and target cybercriminals' infrastructure and finances.

Take Action and Disrupt

Take actions balanced between judicial outcomes and actionable cyber operations.

Evaluate and Assess

Measure the effectiveness of its activities against malicious actors and use this understanding to adapt to emerging threats and technologies.

The FBI's Ransomware Strategy

The FBI's ransomware strategy, finalized in 2023, focuses on targeting the actors, infrastructure, and finances that comprise and enable the ransomware ecosystem. This strategy is organized around four strategic pillars to guide the FBI's overall effort against the ransomware threat. The strategy leverages both the FBI's law enforcement and intelligence authorities to pursue the whole cybercrime ecosystem, including disrupting ransomware groups.

As noted above, in 2022, Congress required creation of the multi-agency JRTF to focus federal efforts to address the ransomware threat. The FBI co-leads the JRTF with the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency; because the JRTF was formally established in 2022, we did not assess the JRTF's ransomware efforts as part of this audit. However, FBI officials noted that the JRTF's Strategic Coordination Group expressed support of the FBI's ransomware strategy and began incorporating elements of the strategy into the JRTF's approach for interagency investigative efforts. Specifically, the FBI has a lead role in the JRTF Investigations and Operations working group, which was focused on four interagency investigative efforts for ransomware in 2023.

According to the Department, the FBI's ransomware strategy has received the support of both the Joint Ransomware Task Force and the National Security Council and, as such, now reflects a whole-of-government approach to the threat.

Significant FBI Ransomware Disruptions

The FBI's strategy contributed to the success of three significant disruptions of ransomware groups in 2023 and early 2024. The FBI defines a disruption as interrupting or inhibiting a threat actor, such as ransomware groups, from engaging in criminal or national security-related activity. A disruption is the result of direct actions and may include, but is not limited to, the arrest, seizure of assets, or impairment of the operational capabilities of threat actors.

In February 2024, the Department and the FBI announced the disruption of the LockBit ransomware group. The FBI Director stated that the FBI and its international partners had successfully disrupted the LockBit

criminal ecosystem, which represented one of the most prolific ransomware variants across the globe.[8] The FBI, working in cooperation with other international partners, disrupted LockBit's operations by seizing numerous public-facing websites used to connect to the group's infrastructure, seized control of the group's servers, and developed decryption capabilities to enable victims around the world to restore systems encrypted using the LockBit ransomware variant.

In 2023, the Department and the FBI announced it had disrupted two other ransomware groups: Hive and ALPHV/Blackcat. First, in January 2023, the FBI announced that, in coordination with foreign partners, it had infiltrated the Hive ransomware group's computer networks to seize control of servers and websites that Hive used to communicate with its members, further disrupting the Hive ransomware group's ability to attack and extort victims. The FBI said it also provided over 1,300 decryption keys to victims of the Hive ransomware variant and prevented victims from having to pay $130 million in ransom demands. Then, in December 2023, the FBI announced it had gained visibility into ALPHV/Blackcat's computer network and seized several websites that the group operated. The FBI stated it had also developed a decryption tool for victims affected by the ALPHV/Blackcat variant to restore their systems, saving them from paying ransom demands totaling approximately $99 million.

When announcing these disruptions, the Department and the FBI both underscored the importance of continuing to disrupt ransomware groups. The FBI Deputy Director stated that the FBI is determined in its efforts to defeat and disrupt ransomware campaigns and that helping victims of crime is the FBI's highest priority and is reflected in this disruption and distribution of tools to assist those victimized in decrypting compromised networks and systems. The Deputy Attorney General stated that the Department will continue to prioritize disruptions and place victims at the center of its strategy to dismantle the ecosystem fueling cybercrime.[9]

The Department's Response to the Ransomware Threat Has Evolved but Opportunities for Improvements Remain

In the following sections, we examine two opportunities where the Department could improve its approach for the ransomware threat based on its activities from 2021 to 2023: (1) whether the Department's metrics for ransomware adequately accounted for the full scope of the Department's efforts to combat ransomware, and (2) whether federal prosecutors and investigators in ransomware cases consistently implemented and complied with the Department's deconfliction policy. Later in this report, we detail our assessment of the NCIJTF Criminal Mission Center's ransomware efforts, which included coordinating whole-of-government plans for ransomware variants in 2021 and 2022.[10]

---

[8] The United States and United Kingdom Disrupt the LockBit Ransomware Variant, Press Release, February 20, 2024. https://www.justice.gov/opa/pr/us-and-uk-disrupt-lockbit-ransomware-variant

[9] The Department of Justice Disrupts the Prolific ALPHV/Blackcat Ransomware Variant, Press Release, December 19, 2023. https://www.justice.gov/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant

[10] The NCIJTF is led by an FBI official who serves as the NCIJTF Director. The NCIJTF structure includes three mission centers – the National Security Mission Center, Digital Innovation Mission Center, and Criminal Mission Center.

The Department's Ransomware Agency Priority Goal

In July 2022, the Department established an Agency Priority Goal for DOJ on combatting ransomware attacks. The Agency Priority Goal, which covered the 2-year period between fiscal years (FY) 2022 and 2023 and ended on September 30, 2023, focused on increasing the response to reported ransomware incidents and the number of seizures or forfeitures in ransomware cases.[11] According to Department officials, the FBI was the primary component responsible for tracking and reporting data on the goal. We reviewed data the FBI collected and provided to the Department for FY 2022.

The first metric measured the speed of the FBI's response to ransomware incidents.[12] While we reviewed the FBI's response to ransomware incident reports, we did not evaluate FBI efforts to assist victims of ransomware incidents. We found FBI field offices initially had limited awareness of the goal, but in October 2022 the FBI Cyber Division sent out communication to improve awareness, state the importance of the metric, and emphasize the need for taking consistent action in response to ransomware incidents. We reviewed a sample of ransomware incident reports created between October 2021 and November 2022 and found that the FBI field office action taken in response to the ransomware incidents generally involved reaching out to victims or conducting database checks. Additionally, we saw that FBI field office action in response to ransomware incidents within 72 hours improved after the FBI Cyber Division communication to the FBI field offices. FBI reported that they had "actioned" (opened, added to existing cases, or resolved) 47 percent of ransomware incidents within 72 hours, for FY 2023, which was an improvement over the 39 percent reported for FY 2022.

Agency Priority Goal – Combat Ransomware Attacks

By September 30, 2023, the Department will enhance its efforts to combat ransomware attacks by:

(1) increasing the percentage of reported ransomware incidents where cases are opened, added to existing cases, or resolved or action taken within 72 hours to 65 percent; and

(2) increasing the number of seizures or forfeitures in ransomware matters by 10 percent.

The second metric measured efforts to increase seizures and forfeitures occurring in ransomware cases. According to a Department official, the FBI had a baseline number of 13 seizures and forfeitures for this metric. We reviewed the FBI data for this metric and found that FBI reported 15 seizures or forfeitures in FY 2022, an increase of 15 percent from the baseline. While the FBI exceeded this metric for FY 2022, Department stakeholders identified concerns about whether it was an effective metric for measuring progress of the Department's efforts to combat ransomware because seizures were largely out of the control of the Department. Specifically, the Department's ability to increase seizures and forfeitures was largely dependent on the specifics of the investigation, which can affect the likelihood of successfully utilizing this type of action.

---

[11] It is unclear whether the Department will keep the ransomware threat a focus of a future Agency Priority Goal. As of May 2024, the Department had not published its action plan or reported any progress for the ransomware Agency Priority Goal on performance.gov, as required by the Office of Management Budget Circular No. A-11, nor has it announced its goals for the next 2-year period covering FYs 2024-2025.

[12] The FBI is notified of a ransomware incident through a variety of sources, such as IC3, and the reports are memorialized in its Guardian system, which is a repository for initial threat information across various domains, including cyber incidents. From this system, the ransomware incidents are assigned to FBI field offices for further action.

In addition, the Agency Priority Goal did not account for the Department's shift from arrests and indictments, which are challenging in ransomware cases, towards those actions to disrupt ransomware actors and the broader cybercriminal ecosystem that enables ransomware to thrive. We believe metrics to track disruptions, such as number of disruptions and measures accounting for providing decryptor keys to victims, represent important additional indicators of the success of efforts against ransomware actors, and the Department should consider tracking similar statistics. Thus, we recommend that the ODAG work with the relevant components to better align metrics across the Department and to determine what metrics for the ransomware threat, including metrics tracking disruption efforts, are most impactful, and which demonstrate the effectiveness of its actions to combat the ransomware threat.

The Department Should Assess its Deconfliction Policy for Cyber Threats to Ensure Consistent Implementation and Compliance

In July 2022, the Department issued its Comprehensive Cyber Review, in which it determined that it needed a policy to ensure that prosecutors and agents take steps at the investigative stage to facilitate early coordination and deconfliction for cyber cases. In February 2023, the ODAG issued a new deconfliction policy for cyber investigations (deconfliction policy).[13] The deconfliction policy was directed at federal prosecutors, requiring them to confirm that federal investigators had conducted deconfliction checks both at the onset of and throughout their investigations. This requirement also applied to cases involving external federal law enforcement investigations. The deconfliction policy laid out a process for federal prosecutors to resolve conflicts, including disputes involving DOJ components or external federal agencies. The process included two steps: (1) attempting to resolve the conflict at the USAO level and coordinating with CCIPS as needed, and (2) elevating the conflict to the ODAG if it remained unresolved.

In January 2024, Criminal Division officials told us that USAOs differed as to their awareness and implementation of the policy. While some USAOs actively worked to deconflict and share information accordingly, others did not share information proactively or cited reasons such as the expansion of discovery obligations for limiting their ability to deconflict. Criminal Division officials acknowledged that deconfliction challenges on ransomware investigations continued to occur, especially for cases involving other federal law enforcement agencies external to the DOJ. For example, an FBI official brought to our attention two ongoing ransomware cases where the FBI experienced difficulties deconflicting with a non-DOJ federal law enforcement agency. According to the FBI, investigators with the non-DOJ federal agency would not share information about its cases with the FBI, affecting the FBI's efforts to properly deconflict its cases and prevent or resolve case overlaps. Further complicating this conflict, the federal prosecutors overseeing these two non-DOJ federal agency cases also would not share information with federal prosecutors handling potentially related FBI ransomware cases to ensure deconfliction occurred as required by the deconfliction policy. The FBI had shared these concerns with CCIPS during their regular meetings on ransomware cases, and CCIPS agreed that the prosecutors in this example were not following the intent of the deconfliction policy.

---

[13] *Guidance Regarding Coordination and Deconfliction of Investigations Involving Cyber and Cyber-Enabled Crimes*, dated February 7, 2023. The ODAG stated that the policy applied to investigations of cyber and cyber-enabled crimes, including crimes where a computer or network is the target of the criminal action (such as ransomware), or where online platforms or digital assets are central to the crime. The Department also incorporated this policy in the Justice Manual Title 9, Section 9-5.1.000 Cyber and Cyber-Enabled Crimes.

In the deconfliction policy, the ODAG stated that the consequences for failing to coordinate and deconflict included 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 the Department. We acknowledge that conflicts are not uncommon in ransomware cases; however, based on anecdotal concerns expressed to us during this audit, we believe that an assessment of the implementation of the deconfliction policy is warranted to ensure consistent implementation and compliance by prosecutors and investigators. Thus, we recommend that the ODAG assess the USAOs' implementation of the deconfliction policy for ransomware cases to ensure that federal prosecutors have a consistent understanding of the policy and comply with its requirements.

Coordination of Multi-Agency Efforts for the Ransomware Threat

Overcoming the threat of ransomware requires collaboration between federal and foreign partners, which includes sharing information and coordinating efforts to combat the threat. In 2021, the Department emphasized that the coordination of ransomware efforts was necessary to ensure that the whole of the U.S. government's resources would be brought to bear to address this threat in a systematic and comprehensive way and that the NCIJTF would help inform the Ransomware Task Force's efforts for this threat. Specifically, the Department identified that the NCIJTF was uniquely situated to plan campaigns to disrupt cyber threats and coordinate interagency action because of its multi-agency participation and collaboration with international and private sector partners. In June 2021, the NCIJTF identified its support of the National Security Council's implementation of the U.S. Counter-Ransomware Campaign Plan, which was the overarching plan for U.S. efforts against ransomware actors and networks.[14] The NCIJTF also developed specific ransomware guidance which designated the NCIJTF's Criminal Mission Center as the NCIJTF lead for coordinating its whole of government ransomware campaigns.

Additionally, in March 2022, Congress required the creation of the multi-agency Joint Ransomware Task Force (JRTF) pursuant to the Cyber Incident Reporting for Critical Infrastructure Act of 2022. The JRTF was established in September 2022 and is led by the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency and the FBI. The JRTF provides strategic direction to U.S. government activities to mitigate and defeat the threat of ransomware on a continuing basis. The JRTF structure includes an Executive Steering Group, Strategic Coordination Group, and various working groups focused on different aspects of the ransomware threat. Because the JRTF was established in 2022, we did not assess its ransomware efforts as part of this audit. Instead, we assessed the Criminal Mission Center's role in coordinating whole-of-government plans for ransomware in 2021 and 2022. We found that the Criminal Mission Center's ransomware role evolved after the creation of the JRTF in 2022 and should be better defined.

[14] The NCIJTF determined that it would leverage its existing coordination framework for whole-of-government campaigns to support this plan, which we refer to as the Campaign Framework.

The NCIJTF Criminal Mission Center Efforts to Coordinate Ransomware Plans in 2021 and 2022

The NCIJTF Criminal Mission Center develops and implements investigative and analytical methodologies to exploit information collected during cyber, criminal, and national security investigations in support of whole-of-government efforts, to include a concentrated effort in the virtual currency space. For the ransomware threat, one of the Criminal Mission Center's key responsibilities was leading operational planning meetings. These meetings were the primary venue for ransomware campaign plans coordination. An objective of these meetings was for agency participants to agree on variants that required whole-of-government campaigns, as well as the identification of lead agencies responsible for executing such efforts. According to NCIJTF officials, the Criminal Mission Center's operational planning meetings led to the development of two ransomware campaign plans: Sodinokibi in September 2021 and Conti in September 2022. However, we found these operational planning meetings stopped occurring and were discontinued in September 2022, which was also around the same time when the JRTF was formally established. Additionally, FBI officials and other stakeholders raised concerns about the Criminal Mission Center's campaign efforts, including what they considered to be inadequate information sharing and communication, a lack of impactful support and outcomes, and an inadequate sense of urgency and capacity to maintain pace with the rapid developments for this threat.

Guidance for Criminal Mission Center Ransomware Plans

U.S. Counter-Ransomware Campaign Plan – The overarching campaign plan for U.S. efforts against ransomware actors and networks.

NCIJTF Campaign Framework – A framework for the coordination of cyber campaigns. A cyber campaign is a formally designated series of focused, coordinated actions, designed to achieve one or more strategic effects through maximum whole-of-government participation.

Ransomware Concept of Operations – Intended as a guide for ransomware campaign coordination roles and responsibilities. Designated the Criminal Mission Center would lead ransomware campaigns efforts at NCIJTF through ransomware operational planning meetings.

Regarding information sharing, while the Criminal Mission Center initially intended to coordinate cross-agency campaigns, an NCIJTF senior official told us that the FBI official assigned to the Criminal Mission Center was unable to facilitate the collaboration necessary to ensure successful ransomware efforts. For example, this individual was excluded from the joint sequenced ransomware operations planned and executed by the FBI's Cyber Criminal Operations Section. The NCIJTF senior official attributed this issue to competing interests between the Criminal Mission Center and the FBI Cyber Criminal Operations Section. Additionally, FBI Cyber Division officials questioned the value of the Criminal Mission Center for whole-of-government campaigns because the Cyber Criminal Operations Section was already focused on joint operational efforts for ransomware. The absence of effective collaboration and resolution of these competing interests, in addition to a lack of clear roles and responsibilities, led to conflict between the two groups.

With respect to the sense of urgency and maintaining pace with the changes to ransomware variants, we found that the Criminal Mission Center developed campaign plans for only two ransomware variants, Sodinokibi and Conti. When the Criminal Mission Center developed those plans, Sodinokibi and Conti represented variants that were highly ranked by the FBI's framework, which as discussed previously, the FBI uses to prioritize variants for disruption. However, by 2023, Sodinokibi and Conti no longer represented the most pressing concern, yet the Criminal Mission Center did not develop additional campaign plans for any other variants.

Regarding impactful outcomes, the Sodinokibi and Conti ransomware campaign plans were the only documentation the Criminal Mission Center could provide in support of its ransomware activities. We reviewed both plans and compared them against the Campaign Framework. According to this framework, campaigns were intended to achieve a series of focused, coordinated, and strategic actions through whole-of-government participation. While the Sodinokibi and Conti plans outlined strategic objectives and actions to achieve them, the Criminal Mission Center could not support whether these strategic objectives had been met or if it had achieved other outcomes in support of the plans. We also found that neither plan identified a lead agency, as required by the Campaign Framework. Additionally, the Campaign Framework stated that all campaigns required termination procedures to conclude the campaign and to produce a final report, regardless of the reason. This final report was to assess the campaign plan and identify lessons learned, ensure any potential outstanding activities and tasks were appropriately assigned, and recommend future actions. While the Criminal Mission Center considered the Sodinokibi plan complete, the status of the Conti plan was unclear. Further, the Criminal Mission Center could not provide a final report or other documentation evidencing either campaign plan's termination. While the Criminal Mission Center intended to coordinate whole-of-government campaigns for ransomware, we found that its efforts did not produce significant results or meaningful outcomes. An NCIJTF senior official and an FBI Cyber Division senior official both agreed with this assessment and confirmed they could not identify a single disruptive action that had originated from the Criminal Mission Center for the ransomware threat.

The FBI Should Better Define the NCIJTF Criminal Mission Center's Role for Ransomware to Ensure its Contributions Are Meaningful and Effective

Subsequent to the creation of the JRTF in 2022, we found the NCIJTF Criminal Mission Center's role for the ransomware threat has evolved and transitioned from a leading role in coordinating whole-of-government ransomware plans to a supporting role for the JRTF. In June 2023, an NCIJTF senior official confirmed that the Criminal Mission Center would no longer lead or exclusively develop additional ransomware campaign plans. Instead, the Criminal Mission Center would support the JRTF's Investigative and Operations working group. FBI officials told us the NCIJTF's future ransomware responsibilities will consist of deconfliction and cryptocurrency analysis; however, neither the FBI nor NCIJTF officials had clearly defined the details of this new role. Therefore, we recommend the FBI, as the responsible body for the NCIJTF, better define the Criminal Mission Center role for ransomware, including how it will support the JRTF to ensure that its contributions are meaningful and effective.

Conclusion and Recommendations

The threat of ransomware attacks and the number of malicious actors conducting ransomware attacks has continued to increase. The Department has worked to counter this threat since 2014, and we found both CCIPS and the FBI, which lead the Department's ransomware efforts, have prioritized the ransomware threat and allocated existing resources in an effort to maximize their impact. However, we found that the Department should assess compliance with its deconfliction policy for cyber investigations to ensure consistent implementation and compliance by federal prosecutors, and that its metrics for ransomware did not account for the Department's important disruption efforts.

We also assessed the NCIJTF Criminal Mission Center's efforts to coordinate whole-of-government ransomware plans in 2021 and 2022 and found it did not demonstrate any meaningful outcomes in response to the ransomware threat. Additionally, we found the Criminal Mission Center's role for ransomware has evolved since Congress created the JRTF in 2022, and that the FBI should better define its role to ensure its support of the JRTF and contributions for ransomware are meaningful and effective.

Ensuring that the Department is improving its coordination and deconfliction efforts will be vital to its success in addressing this escalating threat. Without improvement, the Department risks damaging its investigations and prosecutions, undermining its relationships with victims and domestic and international partners, and becoming less effective at ensuring public safety, national security, and confidence in the Department's abilities in this critical area.

We recommend that the Office of the Deputy Attorney General:

1. Work with the relevant components to better align metrics across the Department and to determine what metrics for the ransomware threat, including metrics tracking disruption efforts, are most impactful, and which demonstrate the effectiveness of its actions to combat the ransomware threat.

2. Assess the USAOs' implementation of the deconfliction policy, for ransomware cases, to ensure that federal prosecutors have a consistent understanding of the policy and comply with its requirements.

We recommend that the Federal Bureau of Investigation:

3. As the responsible body for NCIJTF, better define the Criminal Mission Center role for ransomware, including how it will support the JRTF to ensure that its contributions are meaningful and effective.

APPENDIX 1: Objective, Scope, and Methodology

Objective

The objective of our audit was to assess the Department's strategy to combat ransomware threats, including its coordination and response to ransomware attacks.

Scope and Methodology

The scope of our audit covered April 2021 through September 2023. To accomplish our objectives, we reviewed documentation associated with DOJ's all-tools approach to ransomware, including memoranda, policies, and guidance. We focused on the Department's general approach to combatting ransomware attacks and did not review the Department's specific approach or efforts related to combatting attacks on the Department itself. We reviewed documentation relevant to DOJ's implementation of the Ransomware and Digital Extortion Task Force, including the Federal Bureau of Investigation (FBI) Cyber Division's ransomware strategy. We also reviewed and assessed documentation related to various cases, programs, and task forces that had been undertaken by the Department to address the threat of ransomware. In addition, we assessed Department guidance, including the April 20, 2021, Acting Deputy Attorney General memorandum regarding the Ransomware and Digital Extortion Task Force, and the five strategic areas in the memorandum: enhancing the DOJ's capability to disrupt, investigate, and prosecute ransomware attacks; targeting the ransomware criminal ecosystem as a whole; strengthening the public-private partnerships; working in tandem with federal partners; and furthering collaboration with international partners.

Finally, we gathered and analyzed ransomware-related information from the FBI, Executive Office for U.S. Attorneys (EOUSA), and the National Security Division (NSD). We interviewed officials responsible for the Department's overall approach to addressing threats posed by ransomware within the Office of the Deputy Attorney General (ODAG), the FBI Cyber Division and field offices, and NSD. We also conducted interviews across numerous other DOJ components with mission areas that touch upon or overlap with the ransomware threat, to include: the Criminal Division's Computer Crime and Intellectual Property Section; EOUSA; Money Laundering and Asset Recovery Section; and National Cyber Investigative Joint Task Force's Criminal Mission Center. We spoke with an official from the U.S. Attorney's Office (USAO) regarding their ransomware case and the assistance of and coordination with DOJ entities.

Statement on Compliance with Generally Accepted Government Auditing Standards

We conducted this performance audit in accordance with generally accepted government auditing standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Internal Controls

In this audit, we performed testing of internal controls significant within the context of our audit objectives. We did not evaluate the internal controls of the Department to provide assurance on its internal control

structure as a whole. Department management is responsible for the establishment and maintenance of internal controls in accordance with OMB Circular A-123. Because we do not express an opinion on the Department's internal control structure as a whole, we offer this statement solely for the information and use of the Department.[15]

In planning and performing our audit, we identified several underlying internal control principles within each of the five internal control components that were significant to the audit objectives, including the principle that management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives. As part of our risk assessment, we assessed the design and operating effectiveness of these internal controls and identified deficiencies that we believe could affect DOJ's ability to develop a comprehensive strategy to address the ransomware threat and coordinate on the implementation of its strategy.

The internal control deficiencies we found are discussed in the Audit Results section of this report. However, because our review was limited to those internal control components and underlying principles that we found significant to the objectives of this audit, it may not have disclosed all internal control deficiencies that may have existed at the time of this audit.

Compliance with Laws and Regulations

In this audit we reviewed policies and guidance relevant to ransomware investigations. Our review included the April 2021 Deputy Attorney General memorandum and February 2023 Deputy Attorney General memorandum. We did not test DOJ's compliance with laws or Department guidance, but rather used them as a basis to evaluate DOJ's approach to combatting the ransomware threat.

Sample-Based Testing

To accomplish our audit objective, we performed sample-based testing for Ransomware Guardian Incidents related to the Agency Priority Goal. In this effort, we employed a judgmental sampling design to obtain broad exposure to numerous facets of the areas we reviewed. We reviewed a sample of ransomware incident reports, or "guardians," created between October 2021 and November 2022 and the FBI Field Office action taken in response to the ransomware guardians. This non-statistical sample design did not allow projection of the test results to the universe from which the samples were selected.

Computer-Processed Data

During our audit, we obtained and analyzed ransomware-related case information from DOJ's systems, including the FBI's Sentinel and Guardian systems, and the Criminal Division's case management system. We did not test the reliability of those systems as a whole, therefore any findings identified involving information from those systems were verified with documentation from other sources.

[15] This restriction is not intended to limit the distribution of this report, which is a matter of public record.

APPENDIX 2: The Office of the Deputy Attorney General Response to the Draft Audit Report

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

Office of the Deputy Attorney General

950 Pennsylvania Ave., N.W.
RFK Main Justice Bldg.
Washington, D.C. 20530

MEMORANDUM

TO: Jason R. Malmstrom
Assistant Inspector General
Audit Division
Office of the Inspector General

FROM: Bradley Weinsheimer
Associate Deputy Attorney General
Office of the Deputy Attorney General

DATE: August 30, 2023

SUBJECT: Department of Justice's Response to draft report, "Audit of the Department of Justice's Strategy to Combat and Respond to Ransomware Threats and Attacks"

Thank you for the opportunity to respond to the Office of the Inspector General (OIG) Report titled, "*Audit of the Department of Justice's Strategy to Combat and Respond to Ransomware Threats and Attacks*" (Report), covering April 2021 through September 2023. The OIG Report assesses the Department's strategy to combat ransomware threats, including its coordination and response to ransomware attacks. The Report provides valuable insights to the Department.

As the Report recognizes, combating and responding to the ransomware threat remains one of the Department's top cybercriminal investigative priorities. As indicated in the Report, the FBI and the Department's Computer Crime and Intellectual Property Section (CCIPS) have led the Department's efforts on this front, and they have prioritized their efforts to maximize impact.

As recounted in the Report, since the Department's disruption ten years ago of a botnet used to launch ransomware attacks, the Department has evolved its counter-ransomware strategy to increase use of all available disruption tools and increase coordination to ensure that resources from the whole of government are brought to bear against this threat. The FBI in turn has developed a ransomware strategy that focuses on targeting the whole ecosystem that enables ransomware – a strategy, as the Report notes, that has led to successful and significant disruptions of ransomware groups in the past few years.

In July 2022, as noted in the Report, the Department released its Comprehensive Cyber Review, which included a recommendation that the Department issue coordination and deconfliction policies for cyber investigations to account for the unique nature of the cyber threat. The Office of the Deputy Attorney General (ODAG) followed through in February 2023 by issuing new guidance requiring federal prosecutors to confirm that federal investigators have conducted deconfliction checks before opening ransomware and other cybercrime investigations, and have acknowledged a continuing obligation to conduct such checks during the investigation. The guidance also established procedures for conducting deconfliction. As indicated in the Report, this guidance was later codified in Justice Manual Chapter 9-51.100 ("Cyber and Cyber-Enabled Crimes"). Also in July 2022, as also noted in the Report, the Department issued an Agency Priority Goal for fiscal years (FY) 2022 and 2023 on combating ransomware attacks.

The Report's two recommendations for ODAG focus on ensuring that U.S. Attorney's Offices understand and are complying with the Department's cyber deconfliction policy in ransomware cases, and that metrics used by Department components to measure the impact and effectiveness of counter-ransomware actions are better aligned. We concur with these two recommendations. ODAG will work with the Executive Office for United States Attorneys to assess the implementation of the Department's cyber deconfliction policy at U.S. Attorneys' Offices. ODAG will also continue to work across components to develop metrics that more effectively measure the Department's ransomware disruption activity, and that will align more closely with the disruptive and informative efforts to combat ransomware that are already underway across the Department.

We appreciate OIG's recommendations on this important topic, which has been and remains an important priority of the Department.

APPENDIX 3: The Federal Bureau of Investigation Response to the Draft Audit Report

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D. C. 20535-0001

August 23, 2024

The Honorable Michael E. Horowitz
Inspector General
Office of the Inspector General
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, DC 20530

Dear Mr. Horowitz:

The Federal Bureau of Investigation (FBI) appreciates the opportunity to review and respond to your office's report entitled, Audit of the Department of Justice's Strategy to Combat and Respond to Ransomware Threats and Attacks.

We look forward to working with the Office of the Inspector General to address the recommendation provided in the report. The FBI recognizes the importance in better defining the National Cyber Investigative Joint Task Force, Criminal Mission Center's role when addressing the ransomware threat. The FBI will take corrective action and make necessary improvements. We appreciate your feedback as we continue this effort.

Should you have any questions, feel free to contact me. We greatly appreciate the professionalism of your audit staff throughout this matter.

Sincerely,

Bryan A. Vorndran
Assistant Director
Cyber Division

Audit of the Department of Justice's Strategy to Combat and Respond to Ransomware Threats and Attacks

Recommendation 3: We recommend that the Federal Bureau of Investigation, as the responsible body for NCIJTF, better define the Criminal Mission Center role for ransomware, including how it will support the JRTF to ensure that its contributions are meaningful and effective.

FBI Response: The FBI concurs with the recommendation.

Description of Actions: The FBI, as the responsible body for the NCIJTF, will define a strategy for incorporating the deconfliction requirements laid forth in the *Deputy Attorney General's February 7, 2023 Memorandum Guidance Regarding Coordination and Deconfliction of Investigations Involving Cyber and Cyber-Enabled Crimes*, and the cryptocurrency analytical capabilities of the NCIJTF's Virtual Currency Team, into the operational planning of the JRTF's Investigative and Operations working group.

APPENDIX 4: Office of the Inspector General Analysis and Summary of Actions Necessary to Close the Audit Report

The Office of the Inspector General (OIG) provided a draft of this audit report to the Office of the Deputy Attorney General (ODAG) and Federal Bureau of Investigation (FBI). The ODAG's response is incorporated in Appendix 2 and FBI's response is incorporated in Appendix 3 of this final report. In their responses, the ODAG and FBI concurred with our recommendations and discussed the actions they will implement in response to our findings. As a result, the status of the audit report is resolved. The following provides the OIG analysis of the responses and summary of actions necessary to close the report.

Recommendations for ODAG:

1. **Work with the relevant components to better align metrics across the Department and to determine what metrics for the ransomware threat, including metrics tracking disruption efforts, are most impactful, and which demonstrate the effectiveness of its actions to combat the ransomware threat.**

   Resolved. The ODAG concurred with the recommendation and stated in its response that the ODAG will continue to work across components to develop metrics that more effectively measure the Department's ransomware disruption activity, and that will align more closely with the disruptive and informative efforts to combat ransomware already underway across the Department.

   This recommendation can be closed when the ODAG provides evidence that it worked with the relevant components to better align metrics across the Department and to determine what metrics for the ransomware threat, including metrics tracking disruption efforts, are most impactful, and which demonstrate the effectiveness of the Department's actions to combat the ransomware threat.

2. **Assess the U.S. Attorneys' Offices (USAO) implementation of the deconfliction policy, for ransomware cases, to ensure that federal prosecutors have a consistent understanding of the policy and comply with its requirements.**

   Resolved. The ODAG concurred with the recommendation. The ODAG stated in its response that ODAG will work with the Executive Office for United States Attorneys to assess the implementation of the Department's cyber deconfliction policy at USAOs.

   This recommendation can be closed when the ODAG provides evidence of its assessment of the USAO implementation of the deconfliction policy, for ransomware cases, to ensure that federal prosecutors have a consistent understanding of the policy and comply with its requirements.

Recommendation for the FBI:

3. **As the responsible body for National Cyber Investigative Joint Task Force (NCIJTF), better define the Criminal Mission Center role for ransomware, including how it will support the Joint Ransomware Task Force (JRTF) to ensure that its contributions are meaningful and effective.**

   Resolved. The FBI concurred with the recommendation. The FBI stated in its response that the FBI, as the responsible body for the NCIJTF, will define a strategy for incorporating the deconfliction requirements laid forth in the *Deputy Attorney General's February 7, 2023 Memorandum Guidance Regarding Coordination and Deconfliction of Investigations Involving Cyber and Cyber-Enabled*

Crimes, and the cryptocurrency analytical capabilities of the NCIJTF's Virtual Currency Team, into the operational planning of the JRTF's Investigative and Operations working group.

This recommendation can be closed when the FBI provides evidence documenting that it better defined the Criminal Mission Center role for ransomware, including how it will support the JRTF to ensure that its contributions are meaningful and effective.