HEARING BEFORE THE
COMMITTEE ON THE JUDICIARY
U.S. SENATE

ENTITLED
"RANSOMWARE: UNDERSTANDING THE THREAT AND EXPLORING SOLUTIONS"

MAY 18, 2016

QUESTIONS FOR THE RECORD
FROM CHAIRMAN GRASSLEY TO
DAVID BITKOWER, PRINCIPAL DEPUTY ASSISTANT ATTORNEY GENERAL

- **Can you tell me about what kind of efforts the federal government is taking to prevent ransomware attacks?**

The U.S. government recognizes the serious threat that ransomware poses to businesses, governments and individuals and is actively working to prevent and respond to ransomware schemes. Indeed, the government disseminated detailed C-Suite-level guidance to the health care sector regarding the threat posed by ransomware, how companies can protect their systems against these threats, and how the government can assist should they be victimized. Similar guidance is expected to be released to additional sectors, including to state, local, tribal and territorial partners.

The Department of Justice currently has dozens of active investigations into different ransomware variants and is collaborating with other federal law enforcement agencies on investigations and operations against ransomware schemes. Both the Federal Bureau of Investigation and the Criminal Division participate in an interagency working group to focus on threats created by ransomware. The FBI also operates the Internet Crime Complaint Center to receive reports from victims of ransomware. The Department of Justice regularly shares cyber threat information with Department of Homeland Security (DHS) and works closely with the National Cybersecurity and Communications Integration Center (NCCIC), housed within the DHS, on mitigation efforts related to ransomware and other malware.

The Department of Justice has also led operations to dismantle ransomware schemes and the infrastructure criminals use to spread ransomware and other malware. In 2014, for example, an FBI investigation led to a multi-national effort that disrupted a highly sophisticated ransomware scheme called Cryptolocker, which had encrypted computer files on more than 260,000 computers. Once infected, victims saw a message on their computer monitors, telling them that their files were encrypted and that they had three days to pay a ransom, usually between $300 and $750, if they wanted to receive the decryption key. To dismantle Cryptolocker and the malware that gave it access to victims' computers, the Department and its partners seized computer servers acting as the command and control hubs for the ransomware. The Department

also identified Cryptolocker victims and, working with our partners at DHS, as well as in foreign law enforcement agencies and the private sector, facilitated the removal of malware from many victim computers.

The Department has also been working closely with other federal law enforcement to investigate and prosecute key enablers of ransomware activity. For example, in coordination with the U.S. Secret Service, the Department has disrupted illicit use of major digital currencies such as Liberty Reserve, shutdown global cybercrime organizations, and arrested individuals who facilitated others criminal activities.

The Department also has conducted outreach to educate the public about the threat from ransomware, how to avoid becoming a victim, and what steps one can take to mitigate the harm from ransomware, such as by staying up to date with software patches and making secure back-ups. For instance, FBI published a public service announcement providing tips on how to protect systems from ransomware and respond to infections. In addition, the Cybersecurity Unit within the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS) has issued guidance for organizations and other potential victims of cybercrime, encouraging them to develop incident response plans that can mitigate the damage should they suffer intrusion cyber incident and improve notification of law enforcement agencies. The Department is certainly not alone in public outreach and education campaigns. The U.S. Secret Service, for instance, has provided information and tips on ransomware via its Electronic Crime Task Forces (ECTF), which are located throughout the country.

The Department's outreach efforts also extend across boundaries to international partners. Strong international collaboration and coordination are essential to identifying, disrupting, and mitigating the effects of cyber threats like ransomware. By sharing information and working together with foreign partners, other countries' law enforcement authorities can make arrests, execute search warrants and gather evidence, and seize and disrupt command and control servers and other infrastructure. To support these efforts, the Department works closely with Europol's Cybercrime Centre (EC3) and partner agencies. The Department receives critical, real-time assistance from foreign counterparts through the 24/7 Points of Contact Network established by the Group of Seven Nations and by the Budapest Convention on Cybercrime. The Criminal Division's Office of International Affairs provides invaluable legal support to evidence collection and extradition efforts by both U.S. and foreign law enforcement agencies, while CCIPS conducts training programs to help allies develop cybercrime fighting laws and capacity.

Finally, Congress has a significant role to play by updating the law to ensure law enforcement has the tools it needs to protect the public against cyber threats. In particular, the Administration has proposed expanding courts' authority to issue injunctions like the one used in Coreflood to shut down botnets and widespread ransomware schemes. In addition, we support a proposal to amend the Computer Fraud and Abuse Act – the primary federal anti-hacking statute – to close a loophole that currently clearly criminalizes the creation of botnets, but not the sale or rental of botnets to advance criminal schemes. And the Department supports the Supreme Court's action to amend Rule 41 of the Federal Rules of Criminal Procedure to clarify which court should consider warrants to disrupt botnets and other widespread malware such as ransomware.

- **How are you working with under-resourced state and local governments to ensure they do not become victims?**

As noted above, information sharing is a critical element of our efforts to disrupt cyber threats like ransomware, and these efforts include information sharing with state and local governments. In addition to the specific efforts already mentioned, FBI's InfraGard program has disseminated numerous FBI Liaison Alert System (FLASH) reports and Private Industry Notifications (PINs) containing technical information on ransomware threats to tens of thousands of state and local governments and private sector members, and more alerts are currently being drafted. The Multi-State Information Sharing and Analysis Center (MS-ISAC), a private entity that operates with funding from DHS, routinely disseminates actionable information about cyber threats - including indicators, mitigation steps, and vulnerabilities - to state and local partners. In addition, the FBI, the United States Secret Service, and the MS-ISAC co-hosted open houses in cities throughout the country during the summer of 2016 that provided detailed briefings on cyber threats, prevention and mitigation strategies, and incident response best practices. The event was accessible to state and local governments, as well as private industry and the public. If private or public sector entities, including state and local government agencies, fall victim to ransomware (or any malware for that matter), the federal government has resources to assist: the FBI can deploy criminal investigators and forensic teams to investigate the intrusion and work on identifying the perpetrators, and DHS, among other activities, can deploy assets such as the United States Computer Emergency Readiness Team (US-CERT) to help victims respond to and mitigate the threat.

- **Would you support increased funding for state and local governments to improve their IT infrastructure and prevent cyberattacks – whether ransomware or any other variety?**

Cyber threats of all stripes, including ransomware, continue to grow more prevalent, more sophisticated, and more destructive. Given the severity of these threats to governments, critical infrastructure, and average Americans, it is imperative to ensure that the public and private sectors, including state and local governments, are able to protect their networks and systems, thwart attacks, and respond when intrusions do occur. It is also critical to assist state and local law enforcement agencies so they are prepared to respond, investigate, and prevent ransomware crimes. Programs like the U.S. Secret Service's National Computer Forensics Institute (NCFI), for example, help strengthen the capacity of state and local cyber law enforcement agencies, which collaborate with federal investigators to combat cybercrimes such as ransomware.

- **The President set up a Cybersecurity Commission as part of his Cybersecurity National Action Plan. Do you agree that this Commission should make ransomware prevention a key focus of its investigation and recommendations?**

The Attorney General has made clear that cyber threats such as ransomware, and malware in general, pose a significant danger to public safety and our national security. The Administration

believes that developing detailed recommendations for such dangers are within the Commission's scope.