United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

October 17, 2019

The Honorable Gene Dodaro
Comptroller General of the United States
U.S. Government Accountability Office
441 G Street NW
Washington, D.C. 20548

Dear Mr. Dodaro:

Ransomware[1] is a serious and growing threat to government operations at the federal, state, and local level. According to security research by McAfee, ransomware attacks grew by 118 percent in the first quarter of 2019.[2] Unfortunately, this type of cyberattack is becoming increasingly sophisticated and popular among cyber criminals. The number of reported incidents across the nation where bad actors have attempted to profit from holding state and local government agencies' data hostage is an alarming trend and of great concern to the Committee.

In July 2019, the Department of Homeland Security's Cyber and Infrastructure Security Agency (CISA), Multi-State Information Sharing and Analysis Center, National Governors Association, and National Association of State Chief Information Officers issued a joint statement about the recent outbreak of ransomware attacks.[3] These organizations noted that prevention is the most effective defense against ransomware and identified immediate steps that state and local governments should take to enhance their defensive posture against such attacks. Further, in August 2019, CISA's *Strategic Intent* document noted that the agency intends to use its insight, expertise, capabilities, and reach to assist state and local government partners in improving their cybersecurity posture and defending against the outbreak of ransomware.[4]

We seek a review by the Government Accountability Office to describe federal efforts to assist state and local government entities in protecting their networks and systems from the threat of ransomware and in responding to ransomware incidents. This review should also evaluate

---

[1]Ransomware is a type of malware that targets critical data and systems for the purpose of extortion. The malware attempts to deny access to a user's data, usually by encrypting the data with a key known only to the hacker who deployed the malware, until a ransom is paid.

[2]*See* CHRISTIAAN BEEK ET AL., MCAFEE LABS THREATS REPORT (Aug. 2019), available at https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-aug-2019.pdf.

[3]Press Release, Cybersecurity and Infrastructure Security Agency, CISA, MS-ISAC, NGA & MASCIO Recommend Immediate Action to Safeguard Against Ransomware Attacks (July 29, 2019), available at https://www.us-cert.gov/sites/default/files/2019-07/Ransomware_Statement_S508C.pdf.

[4]*See* CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY, STRATEGIC INTENT (Aug. 2019), available at https://www.dhs.gov/sites/default/files/publications/cisa_strategic_intent_s508c_0.pdf.

whether federal agencies involved in these efforts are effectively coordinating with each other. We appreciate your prompt attention to this matter.

Please contact Harlan Geer of my staff at (202) 224-1497 to discuss the details and timing of this GAO review.

Sincerely,

Maggie Hassan

Margaret Wood Hassan
Ranking Member
Subcommittee on Federal
Spending Oversight and
Emergency Management