Question#:	1
Topic:	Guidance to States
Hearing:	Cracking Down on Ransomware: Strategies for Disrupting Criminal Hackers and Building Resilience Against Cyber Threats
Primary:	The Honorable Carolyn B. Maloney
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

Question: How will the Cybersecurity and Infrastructure Security Agency make sure it provides guidance to state and local governments that reflects the changing ransomware landscape and evaluates cybersecurity plans based on the best information available?

Response: The Cybersecurity and Infrastructure Security Agency (CISA) is focused on reducing the risk of ransomware attacks by working collaboratively with our federal, state, local and private sector partners both to enhance cybersecurity against today's threats and to shape the strategic environment over the long-term. In particular, CISA is working to raise awareness and promote basic cyber hygiene across government agencies at all levels of government, including state and local.

In July 2021, the U.S. Department of Homeland Security led the interagency development and launch of StopRansomware.gov, the U.S. Government's official repository for resources from across the interagency community to help public and private organizations tackle ransomware more effectively. Victims are encouraged to visit "StopRansomware.gov" to help determine if they have been hit by ransomware, learn more about what they can expect as an attack evolves, and see what steps they can take to mitigate the impact. CISA has also made resources available through the Federal Virtual Training Environment, which provides free online cybersecurity training to federal, state, local, tribal, and territorial government employees, federal contractors, and US military veterans.

CISA aims to give state and local governments the tools and guidance they need to increase their resilience and security. CISA continually develops and shares a variety of resources – including extensive guidance and best practices – that can help at-risk entities reduce the chance of being successfully attacked and mitigate the impact if they are attacked. This includes technical indicators related to specific ransomware campaigns. State and local governments can utilize these resources to expand their awareness of ransomware and other cyber threats, assess their individual risk profile, and take positive action to protect themselves against a cyberattack. These resources are free and available through StopRansomware.gov. There are also CISA cybersecurity advisors and coordinators deployed across the country who can help entities at the state and local level connect with CISA cybersecurity products and services.

Question#:	2
Topic:	Useful Information
Hearing:	Cracking Down on Ransomware: Strategies for Disrupting Criminal Hackers and Building Resilience Against Cyber Threats
Primary:	The Honorable Carolyn B. Maloney
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

Question: What specific information from ransomware victims would be most useful for the federal government to guide prevention, detection, and remediation of ransomware attacks?

Response: The most important information for ransomware victims to share is timely and actionable information. Without timely notification to CISA, critical analysis, mitigation guidance, and information sharing is severely delayed, leaving critical infrastructure vulnerable. Rapid reporting of cyber incidents can be the difference between containing an incident and seeing its effects cascade across sectors and the economy. CISA asks that entities experiencing a ransomware incident share information quickly to reduce risk, increase resilience, and aid in response, recovery, and restoration efforts.

When reporting a ransomware attack, victims should share whatever information they currently have at their disposal to receive the most timely and relevant assistance and provide regular updates as the situation develops. CISA requests that any entity reporting an incident specify when the activity was reported; the current level of impact on organizational functions or services; the type of information lost, compromised, or corrupted; an estimated scope of time and resources needed to recover from the incident; the number of systems, records, and users impacted; the network location of the observed activity; and point of contact information for additional follow-up. Victims of ransomware may also consider providing which systems were impacted; the systems and accounts involved in the initial breach; and any relevant logs or samples of any “precursor” malware binaries and associated observables or indicators of compromise. This cyber incident data serves as a critical source of information for risk-based decision-making and the prioritization of assistance, resources and efforts.

Question#:	3
Topic:	Insurance Payouts
Hearing:	Cracking Down on Ransomware: Strategies for Disrupting Criminal Hackers and Building Resilience Against Cyber Threats
Primary:	The Honorable Carolyn B. Maloney
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

Question: Does the insurance industry share information with you about specific policy payouts of a ransom? If yes, how extensive is the data they share? If no, how can we improve information sharing from the insurance industry?

Response: Insurance is regulated at the state level, so it is challenging to broadly determine how much cyber insurance companies are paying for ransomware attacks, or to collect data from them.

The percentage of ransomware incidents potentially unreported to federal law enforcement remains high. We know that private companies are performing incident response work with entities affected by ransomware, and we know that the number of ransomware attacks targeting private companies is on the rise. Today, CISA only receives information on a fraction of incidents. This hampers our ability to conduct critical analysis, spot adversary campaigns, release mitigation guidance, and provide timely response, thus leaving critical infrastructure vulnerable.

Without prompt notification to CISA, critical analysis, mitigation guidance, and information sharing is severely delayed, leaving critical infrastructure vulnerable. Timely information can be the difference between containing an incident and seeing its effects cascade across sectors and the economy. That is why rapid reporting of cyber incidents by private sector entities is crucial. They can help identify significant incidents in their early stages and allow CISA to help mitigate impacts to critical infrastructure before it is too late. Cyber incident data provides insight into current and historical activity.

CISA appreciates the work of members of Congress in both the House and the Senate on cyber incident notification legislation over the past several months. The earlier that CISA, the Federal lead for asset response, receives information about a cyber incident, the faster it can conduct urgent analysis and share information to protect other potential victims. And receiving that information directly from the victims rather than filtered through third party insurers is more likely to result in a fulsome image of any given incident.

Question#:	4
Topic:	Recovery Aspect
Hearing:	Cracking Down on Ransomware: Strategies for Disrupting Criminal Hackers and Building Resilience Against Cyber Threats
Primary:	The Honorable Carolyn B. Maloney
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

Question: The Committee's investigation of ransomware attacks against three private companies has shown that although companies may consider the availability of backup databases in determining whether to pay a ransom, even companies that have a backup database may pay a ransom to resolve an attack more quickly, or as a hedge against potential loss of data. How can we strengthen the "recovery" aspect of ransomware attack response, so that organizations do not feel pressure to pay ransom and can quickly restore their systems?

Response: As a first point, CISA strongly recommends against paying any ransom to cyber-crime organizations or malicious cyber actors. As to the recovery phase of a ransomware attack, CISA recommends that defenders remain focused on cybersecurity holistically, not just the recovery phase because the easiest recovery is from an incident that was prevented from even happening.

Ransomware is a critical challenge and the risks it poses to our Nation's critical infrastructure are severe. However, these challenges are not insurmountable. Ransomware intrusions generally do not use zero-day vulnerabilities or exquisite tradecraft, but rather exploit known security weaknesses or a failure to adopt generally accepted best practices. By investing in stronger cybersecurity, as recommended by CISA, organizations can reduce the risk of a ransomware intrusion and limit related potential impacts.

Specific to recovery, data backups are crucial to minimize the impact of a ransomware incident if data is lost, corrupted, infected, or stolen. CISA recommends that organizations frequently make and store backups of their systems on separate devices that cannot be accessed from a network, such as external hard drives.

The recent high-profile ransomware attacks the country has faced must serve as an urgent call to action to address our nation's cybersecurity risks. We must collectively and with great urgency strengthen our nation's cyber defenses, invest in new capabilities, and change how we think about cybersecurity, recognizing that all organizations are at risk, and we must focus on ensuring the resilience of essential services. Going forward, CISA will continue sharing information about indicators of compromise, tactics, techniques, and procedures, and best practices to reduce the risk of ransomware across sectors. There are multiple new products in the planning process to this end and we look forward to sharing them with you as they are published.

Question#:	5
Topic:	Monitoring Threats
Hearing:	Cracking Down on Ransomware: Strategies for Disrupting Criminal Hackers and Building Resilience Against Cyber Threats
Primary:	The Honorable Gerald E. Connolly
Committee:	OVERSIGHT & GOV RFORM (HOUSE)

Question: As the Sector Risk Management Agency (SRMA) for nine critical infrastructure sectors, how does the Department of Homeland Security quantify, baseline, and continuously monitor the specific cybersecurity threats across each sector for which you are the SRMA? How do you maintain visibility of each sector's cyber health?

Response: Efforts to maintain situational awareness regarding the cyber posture of the different sectors must rely on robust collaboration and open dialogue with the corresponding critical infrastructure sector partners. A vibrant public-private partnership represents the foundation for any approaches focused on understanding and characterizing the cybersecurity health and maturity of the sectors. Each one of the critical infrastructure sectors for which CISA performs the corresponding Sector Risk Management Agency (SRMA) responsibilities has unique characteristics, operating models, and risk profiles. Accordingly, CISA facilitates public-private collaboration structures across these sectors to develop strategic goals to mitigate risks and improve resilience; promote education, training, and information sharing on threats and vulnerabilities; and provide technical assistance and recommendations regarding monitoring of threats, identification of vulnerabilities, mitigation of impacts, and post-incident recovery. This is done under the auspices of an all-hazards approach that recognizes the broad spectrum of threats that are relevant to critical infrastructure.

The execution of CISA's responsibilities as the SRMA for the assigned sectors spans different types of activities, conducted by multiple divisions and offices. Monitoring of threats and identification of vulnerabilities benefit from the multi-stakeholder interactions and knowledge exchange that take place under these lines of effort. In turn, any consensus advice or recommendations from the public-private partnership informs those activities to better align them with the risk landscape that is particular to each critical infrastructure sector.