Question#:	1
Topic:	Expanding Services
Hearing:	America Under Siege: Preventing and Responding to Ransomware Attacks
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: Will CISA be expanding its services to businesses as the threat of ransomware grows? I understand stopransomware.gov to be a first step. What is the next step? Are you also looking into, for example, expanding phone support for small business and individuals, or providing cybersecurity products directly?

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 to enhance infrastructure cybersecurity against today's threats and shape the strategic environment over the long-term. CISA is engaged on multiple fronts to help address ransomware and is working to raise awareness and promote basic cyber hygiene across tens of thousands of businesses and within our own government agencies. In summer 2021, CISA 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 through the arc of the attack, and see what steps they can take to mitigate the impact and to recover.

CISA aims to give organizations the tools and guidance they need to increase their resilience and security. We continually develop and share 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. Entities 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 from a successful cyberattack. These resources are free and available through "StopRansomware.gov".

CISA is also available to provide technical assistance, upon request, to critical infrastructure organizations during major cybersecurity incidents. CISA's role is to help victims understand the extent of an intrusion, evict the adversary, adopt strong security practices to prevent future intrusions, and also to gather information to protect other potential victims from being attacked in the first place. CISA has cybersecurity advisors and coordinators deployed across the country who offer cybersecurity assistance on a voluntary, no-cost basis to critical infrastructure organizations, including state, local, tribal and territorial (SLTT) governments. The cybersecurity advisors and coordinators provide cyber preparedness, strategic messaging, working group support, partnership development, cyber assessments, threat information sharing and incident coordination and support. As an example, during a recent ransomware incident involving the food/agriculture sector, cybersecurity advisors partnered with CISA headquarters, private sector

Question#:	1
Topic:	Expanding Services
Hearing:	America Under Siege: Preventing and Responding to Ransomware Attacks
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

partners associated with the Joint Cyber Defense Collaborative, and the Federal Bureau of Investigation (FBI) to mitigate the ransomware attack and restore their systems to continue their business operations.

Additionally, CISA is building new, and strengthening existing, partnerships with key players to leverage its expansive information-sharing authorities to ensure early warning of threats and attacks.

Question#:	2
Topic:	Cyber Insurance
Hearing:	America Under Siege: Preventing and Responding to Ransomware Attacks
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: How useful is cyber insurance for large business and local governments? Is cyber insurance an essential expense for small businesses?

Does cyber insurance result in more ransoms being paid, which can have the unwanted effect of increased funding to criminal groups?

Response: Cyber insurance is a relatively new and specialized market that broadly includes forms of insurance that address losses resulting from cybersecurity or other computer-related issues, depending on the coverage. Although cyber insurance products have been on the market since the late 1990s, the market is still maturing and remains underdeveloped despite significant growth over the last two years. This relatively new form of insurance varies greatly from carrier to carrier in terms of coverage, as well as how carriers measure and assess risk.

SLTTs and private sector partners have availed themselves of cyber insurance for several years. Organizations participate in the cyber insurance market to transfer the risk of cyber threats. However, there are multiple issues limiting the potential of the cyber insurance market and the pace at which the market is evolving, namely the ability to assess risk accurately. To do so, insurance companies would need to mature underwriting guidelines, risk management processes, and robust and reliable pricing models that are continuously validated, especially given the dynamic nature of cyber risk.

Question#:	3
Topic:	Agriculture Ransomware
Hearing:	America Under Siege: Preventing and Responding to Ransomware Attacks
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: Agriculture is a target for ransomware. What are some of the unique challenges of protecting agriculture from these attacks?

Response: In addition to the negative impacts faced by other businesses, ransomware attacks targeting the agriculture sector can also impact the food supply chain, resulting in direct consequences for every American. The introduction of information technology to the industry brings cybersecurity requirements to large businesses, small farms, and producers that may not have considered these risks before now. Taking recommended steps to protect networks, systems, and data may be difficult to manage for small-scale operations that have limited resources and experience implementing and managing cybersecurity programs. Additionally, the geographically distributed nature of agriculture in the U.S. makes identifying, detecting, remediating, and recovering from cybersecurity-related issues particularly challenging. While small farms and producers may not be a primary target, these groups represent a significant part of the industry, increasing risk and the challenge of mitigating cybersecurity issues at scale. CISA's resources listed on "StopRansomware.gov" are designed to be accessible to businesses of different sizes and levels of cybersecurity experience, with many products specifically designed for small and medium businesses.

Question#:	4
Topic:	Unreported Incidents
Hearing:	America Under Siege: Preventing and Responding to Ransomware Attacks
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: During the hearing you noted that you believe that only about a quarter of ransomware incidents are reported.

Can you please confirm the percentage of ransomware incidents that are believed to be unreported to federal law enforcement? Please describe how you arrived at your estimate.

Why do you believe so many incidents are unreported? Are any of these incidents reported to state or local law enforcement but not federal law enforcement?

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

CISA must continue to invest in and mature our voluntary partnerships with critical infrastructure entities. Ensuring that partners are aware of information sharing protections available through the Cybersecurity Information Sharing Act of 2015 and the Protected Critical Infrastructure Information Act will help enhance trusted information sharing between CISA and the private sector. We further look forward to working with Congress in enacting mandatory incident reporting legislation.

Question#:	5
Topic:	Reporting Mandate
Hearing:	America Under Siege: Preventing and Responding to Ransomware Attacks
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: If Congress mandates reporting of ransomware incidents to federal law enforcement, what incentives or penalties does CISA recommend be included in the mandate to promote compliance?

If Congress mandates reporting of ransomware incidents, to what agencies does CISA recommend reporting to satisfy a mandate?

Response: CISA appreciates Congress's leadership on this issue and applauds the recent passage of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRA"), which became law with the Fiscal Year 2022 Omnibus Appropriations bill. This legislation enables the visibility required for us to better see cybersecurity threats and to address the devastating effects of cyber-attacks.

The reality is that the private sector owns and operates the vast majority of our nation's critical infrastructure, so they play a vital role in working with CISA to improve our nation's cybersecurity. Mandatory incident notification is necessary for CISA and other federal agencies to identify significant incidents in their early stages and allow us the window needed to analyze the situation and then investigate, respond to the adversary, and help mitigate impacts. CISA supports broad cyber incident reporting requirements that would require the reporting of a range of cyber incidents, including ransomware and incidents that impact critical infrastructure and their supply chains.

Over the next 24 months, CISA will develop proposed rules for implementing mandatory cyber incident reporting for critical infrastructure owners and operators. The rulemaking process will be consultative with our government and industry partners and will ensure that we are striking the right balance between getting accurate information quickly and letting victims respond to an attack without imposing onerous requirements on them. Part of this rulemaking process will include the establishment of thresholds of impact to ensure that the information received is relevant and impactful.

CISA and its partners, such as the FBI, will use these reports to build a common understanding of how our adversaries are targeting U.S. networks and critical infrastructure. This information will fill critical information gaps and allow us to analyze incoming reporting across sectors to spot trends, deploy resources and render assistance to victims suffering attacks, and quickly share that information with network defenders to warn other potential victims. These reports will help identify significant incidents in their early stages and allow us to help mitigate impacts to critical infrastructure.

Question#:	5
Topic:	Reporting Mandate
Hearing:	America Under Siege: Preventing and Responding to Ransomware Attacks
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

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. CISA's goal is not to overwhelm companies or our own personnel, but to balance getting information in a timely manner with ensuring that information is meaningful and actionable. Any mandated reporting of cybersecurity incidents should include timely reporting to CISA, along with any other departments and agencies the Administration and legislation determines appropriate. .

Question#:	6
Topic:	Agency Coordination
Hearing:	America Under Siege: Preventing and Responding to Ransomware Attacks
Primary:	The Honorable Charles E. Grassley
Committee:	JUDICIARY (SENATE)

Question: How do FBI, USSS, and CISA coordinate among agencies to ensure efforts are not duplicated?

Response: Every incident is unique and requires a high degree of interaction with the affected entity to determine incident severity and impact, among other technical details necessary for incident response.

Under Presidential Policy Directive (PPD) 41, CISA serves as the lead for asset response during a significant cyber incident. As the lead for asset response, CISA is focused on helping victim organizations evict the adversary and restore to a secure state. CISA also aims to derive information from the intrusion to share quickly with government and private sector partners to understand the extent of the threat and recommend actions that will help prevent further similar intrusions. CISA collaborates with industry and government partners to help organizations understand and counter cybersecurity risks associated with the malicious activities of nation-state and non-state actors. FBI is the lead agency for threat response activities, focused on investigating an incident, attributing incidents to adversaries and contextualizing them within the broader threat intelligence picture, and working with federal and foreign partners to impose costs on the responsible actor. The United States Secret Service (USSS) provides critical investigatory capabilities under its unique authorities.

CISA also has cybersecurity advisors and coordinators deployed across the country who offer cybersecurity assistance on a voluntary, no-cost basis to critical infrastructure organizations, including SLTT governments. The field-based cybersecurity advisors and coordinators partner with their local FBI and USSS field offices to provide cyber preparedness, strategic messaging, working group support, partnership development, cyber assessments, threat information sharing, and incident coordination and support.

CISA's success in its mission relies on building strong partnerships to collectively address our shared risk. Cybersecurity requires a whole-of-government and whole-of-society approach. CISA is focused on working with its interagency partners to ensure accountability in managing, mitigating, and reducing risk to digital and critical infrastructure.

Question#:	7
Topic:	OFAC Designations
Hearing:	America Under Siege: Preventing and Responding to Ransomware Attacks
Primary:	The Honorable Ben Sasse
Committee:	JUDICIARY (SENATE)

Question: Given the growing frequency of high-profile ransomware attacks and given that the main prohibition on ransomware payments only relates to payments made to OFAC designated entities, why are we not seeing more sanctions on these variants?

Response: USSS works closely with the Office of Foreign Assets Control (OFAC) of the U.S. Department of the Treasury, and other relevant interagency partners, to consider the potential applications of sanctions under Executive Order 13694 and related authorities. OFAC publishes identifying information of individuals, groups, and entities that are specially designated for sanctions. Publicly identifying such foreign persons or entities has the potential of impeding law enforcement and other actions against them by causing them to go in to hiding or otherwise altering their operations so they can continue their criminal activity. Therefore, interagency consideration is essential to effectively and appropriately use sanctions designations to address malicious cyber activity.

Question: To what extent have each of your agencies observed a change in the character, makeup, and activity of any ransomware variants that have previously been designated by OFAC?

Response: The USSS has observed foreign persons designated for their malicious cyber activities continue to engage in similar transnational cyber criminal activity.

Question: Should public attribution inherently lead to OFAC designations?

Response: If the U.S. government has already publicly identified foreign persons engaging in malicious cyber activity, such as by unsealing an indictment, then OFAC also designating them likely presents little additional operational risk. However, further consideration may be warranted to determine if sanctions are appropriate and consistent with relevant laws, including the International Emergency Economic Powers Act (50 U.S.C. 1701 *et seq*.) (IEEPA), the National Emergencies Act (50 U.S.C. 1601 *et seq*.) (NEA), and/or section 212(f) of the Immigration and Nationality Act of 1952 (8 U.S.C. 1182(f)). To this end, the interagency deliberates and sequences whole-of-government campaigns including a range of cost-imposing consequences against adversaries. These decisions are made necessarily on a case-by-case basis in an effort to shape adversary behavior in light of what we know about adversary motivations through intelligence, diplomatic, law enforcement, economic, and CERT-to-CERT channels.

Question: Please describe the law enforcement challenges associated with bringing these variants to justice without sanctions.

Question#:	7
Topic:	OFAC Designations
Hearing:	America Under Siege: Preventing and Responding to Ransomware Attacks
Primary:	The Honorable Ben Sasse
Committee:	JUDICIARY (SENATE)

Response: Ransomware variants are easily created, therefore the USSS focuses on arresting and seizing the assets of those involved in criminal conspiracies and other violations of federal law. Often these individuals reside in foreign countries and it requires significant international law enforcement cooperation to locate and extradite them to face justice. In cases where ransomware actors are located in countries without an extradition treaty with the United States and poor mutual law enforcement assistance relationships, such as Russia, law enforcement often witnesses criminals enjoying “safe haven” wherein they can operate with relative impunity from local justice. Despite the challenges inherent in such operations, the USSS and our law enforcement partners have been successful in arresting such individuals. This includes those that are located in countries that do not have extradition treaties with the United States. Developing the investigative teams and international cooperation to scale these law enforcement efforts to curb the growing threat of ransomware is an important budgetary priority, which is challenging to execute under a continuing resolution and fiscal uncertainty.The FBI can provide additional insight on the range of challenges faced by law enforcement.

Question#:	8
Topic:	Deterrence
Hearing:	America Under Siege: Preventing and Responding to Ransomware Attacks
Primary:	The Honorable Ben Sasse
Committee:	JUDICIARY (SENATE)

Question: How do each of your respective agencies think about deterring actors in this space?

What have you found to be the most valuable tools to deter average cybercriminals and ransomware variants from launching attacks?

Where are the most prominent limits to deterrence theory in practice?

Response: CISA focuses on driving "deterrence through denial," in which targeted organizations adopt strong security and resilience measures to make it difficult for cyber adversaries to achieve their goals. CISA develops and shares 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, including technical indicators related to specific ransomware campaigns. ”StopRansomware.gov” provides cyber incident preparedness resources, including checklists and training to help organizations reduce the likelihood of becoming a victim of a ransomware attack and guides on what to do if affected by ransomware, directing readers to a reporting mechanism to the FBI, CISA, and the USSS. Organizations should apply these best practices to the greatest extent possible based on the availability of organizational resources to help manage the risk posed by ransomware and support a coordinated and efficient response to a ransomware incident.

Question#:	9
Topic:	Ransomware Insurance I
Hearing:	America Under Siege: Preventing and Responding to Ransomware Attacks
Primary:	The Honorable Ben Sasse
Committee:	JUDICIARY (SENATE)

Question: How would you describe the role of the ransomware insurance market in combatting the growing ransomware issue? Is the insurance market more helpful or harmful to the ultimate goal of reducing ransomware attacks?

Are companies with ransomware insurance more likely to pay a ransom than those without insurance?

Is there any evidence to suggest that hackers are more likely to target companies that have ransomware insurance?

Response: Cyber insurance is a relatively new and specialized market that broadly includes forms of insurance that address losses resulting from cybersecurity or other computer-related issues, depending on the coverage. Although cyber insurance products have been on the market since the late 1990s, the market is still maturing and remains underdeveloped despite significant growth over the last two years. This relatively new form of insurance involves coverages that vary greatly from carrier to carrier, as well as how carriers measure and assess risk.

SLTTs and private sector partners have availed themselves of cyber insurance for several years. Organizations participate in the cyber insurance market to transfer the risk of cyber threats. However, there are multiple issues limiting the potential of the cyber insurance market and the pace at which the market is evolving, namely the ability to assess risk accurately. To do so, insurance companies would need to mature underwriting guidelines, risk management processes, and robust and reliable pricing models that are continuously validated, especially given the dynamic nature of cyber risk.

Similarly, the limited visibility into the full scope of different ransomware incidents limits the ability to determine if hackers target insured companies over the uninsured. Mandatory incident reporting legislation could provide insight allowing an answer to this question of targeting.

Question#:	10
Topic:	Ransomware Insurance II
Hearing:	America Under Siege: Preventing and Responding to Ransomware Attacks
Primary:	The Honorable Ben Sasse
Committee:	JUDICIARY (SENATE)

Question: According to the blockchain research firm Chainalysis, ransomware payments reached a total of $412 million during 2020, representing a 341 percent increase over the prior year. How is the ransomware insurance market responding to this growing number of attacks?

Are insurance companies requiring their customers to maintain any baseline security or preventative measures in order to qualify for coverage?

Outside of advising on "best practices," is there anything else the government can, or should, be doing to fortify our resilience against ransom attacks through the insurance industry?

Response: Cyber insurance is a relatively new and specialized market that broadly includes forms of insurance that address loses resulting from cybersecurity or other computer-related issues, depending on the coverage. Although cyber insurance products have been on the market since the late 1990s, the market is still maturing and remains underdeveloped despite significant growth over the last two years. This relatively new form of insurance involves coverages that vary greatly from carrier to carrier, as well as how carriers measure and assess risk.

SLTTs and private sector partners have availed themselves of cyber insurance for several years. Organizations participate in the cyber insurance market to transfer the risk of cyber threats. However, there are multiple issues limiting the potential of the cyber insurance market and the pace at which the market is evolving, namely the ability to assess risk accurately. To do so, insurance companies would need to mature underwriting guidelines, risk management processes, and robust and reliable pricing models that are continuously validated, especially given the dynamic nature of cyber risk.

Question#:	11
Topic:	Ransomware Insurance Regulations
Hearing:	America Under Siege: Preventing and Responding to Ransomware Attacks
Primary:	The Honorable Ben Sasse
Committee:	JUDICIARY (SENATE)

Question: Who is currently responsible for regulations relating to the ransomware insurance industry?

At present, are insurance companies required to report to the government ransom attacks against their customers for whom they make payments? If not, is there any reason why they should not be required to do so?

Response: Insurance is regulated at the state level.

Although some sectors (*e.g.*, financial institutions and healthcare) are required under federal law to report to a federal regulator regarding incidents affecting their systems or information, there is currently no single mandatory federal requirement to report cyber incidents or ransomware payments (including payments that insurance companies make on behalf of other entities). Rather, entities must assess the complex disclosure requirements imposed by an array of agencies at the federal and state levels. Moreover, when a victim does seek to do the right thing and report an incident to the federal government, they may not know which agencies to contact, delaying their reporting during an emergency situation. Among the harms this may cause is a lag in availability of critical mitigation guidance to the operators who are positioned to take action. Without timely 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.

CISA appreciates the work of members of Congress in both the House and the Senate on cyber incident notification in the 117th Congress. 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. Further, it would allow insight that could answer these questions on the value of cyber insurance.

Question#:	12
Topic:	Combatting Attacks
Hearing:	America Under Siege: Preventing and Responding to Ransomware Attacks
Primary:	Senator Thom Tillis
Committee:	JUDICIARY (SENATE)

Question: We have heard that combatting ransomware threats requires a whole-of-government and whole-of-society approach. What must be done to improve coordination among the many actors that play a role in combatting ransomware attacks, stopping future attacks, and bringing the bad actors to justice, and what should Congress do to help?

Response: One of CISA's top priorities is forging strong partnerships with critical infrastructure partners to enable robust operational collaboration, identify adversary activity across sectors, produce more targeted guidance, and ultimately reduce the frequency and impact of cyber incidents. We are leveraging these partnerships to increase operational collaboration through the newly established Joint Cyber Defense Collective (JCDC). The JCDC will leverage CISA's broad authorities to share information about threats and vulnerabilities to enable early warning and prevent other victims from being attacked, enabling us to transform information sharing into timely, relevant information action.

The JCDC brings together the authorities, capabilities, and talents of the federal government with the power of industry to enable shared situational awareness of the threat landscape, to plan and action against the most significant threats to the nation. The JCDC leads the development of the nation's cyber defense plans, which outline activities to prevent and reduce the impacts of cyber intrusions. Leveraging new authorities provided by the National Defense Authorization Act of 2021, the JCDC brings together public- and private sector entities to unify deliberative and crisis action planning while coordinating the integrated execution of these plans. The plans promote national resilience by coordinating actions to identify, protect against, and respond to malicious cyber activity targeting U.S. critical infrastructure or national interests.

Question#:	13
Topic:	Private Information Sharing
Hearing:	America Under Siege: Preventing and Responding to Ransomware Attacks
Primary:	Senator Thom Tillis
Committee:	JUDICIARY (SENATE)

Question: What reasons do private sector entities give as to why they may not readily share information with the federal government. What assurances are you prepared to give those who share information or report incidents to address concerns that sharing information with the government could lead to harm to reputation, regulatory retaliation, or harms to private sector intellectual property? How will the government safeguard data provided by companies as part of the effort to combat ransomware attacks?

Response: The private sector, which owns and operates most of the nation's critical infrastructure, plays a vital role in working with CISA to improve our nation's cybersecurity. Private sector organizations are not required to request assistance from the federal government but are strongly encouraged to consider requesting assistance from CISA when faced with a cyber intrusion. Incentivizing the private sector to work with the federal government is key to the voluntary collaboration upon which CISA has always relied. The private sector must see the benefit and the results through efforts such as CISA's assistance programs and threat information sharing programs as outweighing any risk in sharing. It is incumbent on CISA to provide that assurance to our partners. For example, ensuring that partners are aware of information sharing protections available under the Cybersecurity Information Sharing Act of 2015 and the Critical Infrastructure Information Act will enable enhanced trusted information sharing between CISA and the private sector. CISA has discovered that private sector entities are not always aware of the existence of these protections, which can result in less information being shared in a timely manner. In addition, private sector entities often point to European privacy regulations as a reason for why they cannot share cyber threat information with CISA.

Rapid reporting of cyber incidents by private sector entities can help identify significant incidents in their early stages and allow CISA to help mitigate impacts to critical infrastructure. CISA can help an organization determine the scope of the infection, ensure the adversary is out of the network, and advise on how to rebuild -- but only if we know about the incident. CISA provides secure means for constituents and partners to report incidents, phishing attempts, malware, and vulnerabilities. Irrespective of the type of incident or its reporting method, CISA works to help affected entities understand the incident, link related incidents, and share information to rapidly resolve the situation in a manner that protects privacy and civil liberties.

CISA views privacy as more than just compliance with privacy law and policy. Privacy at CISA is also about public trust and confidence, and how the government acts responsibly and transparently in the way it collects, maintains, and uses information provided by the public. CISA has a long history of receiving information from the private sector and has, throughout that history, effectively protected the data supplied to us by our partners consistent with the principles of the Privacy Act of 1974, the E-Government Act of 2002, and the Critical Infrastructure Act of

Question#:	13
Topic:	Private Information Sharing
Hearing:	America Under Siege: Preventing and Responding to Ransomware Attacks
Primary:	Senator Thom Tillis
Committee:	JUDICIARY (SENATE)

2002. CISA regularly works with the private industry and diligently protects the data and privacy of the entities we work with. We will continue this practice whether information is shared pursuant to voluntary cyber threat information sharing program or, if enacted, under a mandatory incident reporting law. Regardless of how incident information is reported, CISA remains committed to using that information in a way that protects the victim's identity and helps to protect future targets from compromise.

Question#:	14
Topic:	Retention
Hearing:	America Under Siege: Preventing and Responding to Ransomware Attacks
Primary:	Senator Thom Tillis
Committee:	JUDICIARY (SENATE)

Question: What changes need to be made to the federal government or your Department's hiring practices to attract and retain top cybersecurity professionals? How will the planned cybersecurity talent management system and other policy changes under consideration by your agency assist in combatting cybercrimes and ransomware attacks? When will such changes be implemented?

Response: Building the nation’s cyber workforce is a major priority for CISA. Projections suggest a global cybersecurity workforce shortage of millions, with more than half a million of those positions in the U.S. alone. The United States has an estimated 500,000 vacant cybersecurity jobs, over 35,000 within the government. These are high-paying, professional jobs that need people of diverse backgrounds and experiences to fill them!

CISA offers a diverse set of career prospects, from ethical hackers, who are engaged in penetration testing or "red team" attacks, to malware analysts, who study the functionality and potential origins of malware samples, to a host of other positions. CISA strives to prioritize career growth for our workforce. Because the cybersecurity field is so diverse, that are many opportunities to move up, gain more experience, or transfer positions.

On November 15, 2021, DHS and CISA launched the Cybersecurity Talent Management System (CTMS), an innovative new personnel system designed to more effectively recruit, compensate, and retain our top cybersecurity professionals. Through CTMS, the DHS hiring process for cybersecurity positions can shift away from the standard hiring model, which is largely based on formal education requirements, to instead focus on a candidate’s demonstrated skills and aptitude. CTMS candidates will be evaluated by a series of assessments and simulations.

CTMS will be used as an additional tool to attract the full spectrum of cyber talent from entry-level through senior executives, including technical subject-matter experts. CTMS will strengthen the cyber workforce by bringing in applicants from both outside as well as from within the federal government.

CTMS is unique as it completely reimagines the entire federal hiring process. Importantly, it is designed to be adaptable to meet mission and market demands. CTMS will help improve the ability to identify mission critical skills, build a better pipeline to help the best qualified candidates make the transition between the private sector and the government, and compensate team members using market-sensitive salaries based on their demonstrated expertise.

Question#:	15
Topic:	New Website
Hearing:	America Under Siege: Preventing and Responding to Ransomware Attacks
Primary:	Senator Thom Tillis
Committee:	JUDICIARY (SENATE)

Question: The new website StopRansomware.gov is designed to pool resources from several government agencies. What plans are there to ensure that this information is curated, maintained, and remains relevant and user-friendly? What efforts are made to ensure the public is aware of this resource?

Response: "StopRansomware.gov" is a whole-of-government website. As such, CISA works with partners across the federal government to update threat information and ensure it remains relevant. The site is discussed regularly at multiple stakeholder meetings and CISA works with agencies to add information as it becomes available. The website and its resources are also listed in speaking engagements, at conferences and events, and via social media. It is consistently in the top 10 pages visited on CISA.gov and, to date, has been visited more than 454 thousand times.

Question#:	16
Topic:	Resources Available
Hearing:	America Under Siege: Preventing and Responding to Ransomware Attacks
Primary:	Senator Thom Tillis
Committee:	JUDICIARY (SENATE)

Question: What resources are you making available to State and Local Governments in light of the ransomware crisis?

Response: CISA is urgently focused on reducing the risk of ransomware attacks by working collaboratively with all of our partners, including SLTT governments to enhance cybersecurity against today's threats and shape the strategic environment over the long-term to a better protected one.

In January 2021, CISA kicked off a cybersecurity awareness and outreach campaign to encourage public- and private sector organizations and key stakeholders to take appropriate actions to "Reduce the Risk of Ransomware." In coordination with the Multi-State Information Sharing and Analysis Center, CISA released a joint Ransomware Guide that details industry best practices and a response checklist that can serve as a ransomware-specific addendum to state and local governments' cyber incident response plans. CISA supported DHS Secretary Mayorkas' Ransomware Sprint, which ran through April and May 2021 and was designed to ensure that all sectors of the economy, including SLTTs, understand the criticality of this risk and take urgent action in response. CISA has already filled 37 of the Cybersecurity State Coordinator positions based in the 50 state capitals and will fill the remaining spots in the near future as authorized in the Fiscal Year 2021 National Defense Authorization Act. Duties of these state coordinators include: relationship building and advisement on governance structures for developing and maintaining secure and resilient infrastructure; serving as the federal cybersecurity risk advisor to support preparation, response, and remediation efforts; facilitating cyber threat information sharing; raising awareness of federal cybersecurity resources available to non-federal entities to increase resilience; supporting training and exercises, and planning for continuity of operations and expedited recovery; serving as a principal point-of-contact for non-federal entities to engage the federal government on cyber incidents; assisting non-federal entities in developing vulnerability disclosure programs; and assisting in the development of state cybersecurity plans. Augmenting the state coordinators, CISA also has cybersecurity advisors deployed in major cities across the country who offer cybersecurity assistance on a voluntary, no-cost basis to critical infrastructure organizations including SLTTs. These cybersecurity advisors and coordinators force multiply our already substantial regional efforts and the outreach to our SLTT partners will do nothing but increase in the future.

In July, CISA spearheaded the development and launch of the whole-of-government resource "StopRansomware.Gov" to make it easier for organizations across the country to find free and authoritative information, resources, and tools they need to prepare for and respond to ransomware intrusions. The launch of StopRansomware.gov is a reflection of how dangerous the threat of ransomware is – this is a coordinated effort across numerous federal agencies, who are

Question#:	16
Topic:	Resources Available
Hearing:	America Under Siege: Preventing and Responding to Ransomware Attacks
Primary:	Senator Thom Tillis
Committee:	JUDICIARY (SENATE)

pooling their resources to enable organizations to learn how to reduce their ransomware risk and better protect their networks, with the effect of discouraging malicious cyber actors from engaging in ransomware.

Further, CISA is developing a catalog of Bad Practices that are exceptionally risky to encourage organizations to implement an effective cybersecurity program to protect against cyber threats. Sector-specific guidance is also being developed and will be provided for all 16 critical infrastructure sectors vital to the nation. Disabling or destroying the 16 critical infrastructure sectors would cause great harm to security, economic welfare, public health, and safety.

Additionally, CISA has also made resources available through the Federal Virtual Training Environment, which provides free online cybersecurity training to federal employees, SLTT government employees, federal contractors, and US military veterans.

Question#:	17
Topic:	Secure Storage
Hearing:	America Under Siege: Preventing and Responding to Ransomware Attacks
Primary:	Senator Thom Tillis
Committee:	JUDICIARY (SENATE)

Question: What percentage of data is encrypted at rest on federal and commercial systems? How can we incentivize system owners to further adopt secure storage solutions?

Response: As directed by Section 3(c)(ii) of Executive Order 14028, "Improving the Nation's Cybersecurity," CISA is working across the federal civilian executive branch to understand government-wide progress in adopting multifactor authentication and encryption of data at rest and in transit.

Through the Executive Order, CISA will support agencies in driving adoption of multifactor authentication and encryption for data at-rest and in-transit and will also work with NIST to develop an initial list of secure software development lifecycle standards for software purchased by the Federal Government and minimum testing requirements for software source code. CISA will continue to analyze the reporting coming in from the interagency and take appropriate action to maximize the implementation of multifactor authentication and date encryption across the Federal Civilian Executive Branch.

To help with these changes, CISA recently developed a Zero Trust Maturity Model and Cloud Security Technical Reference Architecture to assist agencies as they implement data protection measures by leveraging ZTAs and greater use of the cloud. The Zero Trust Maturity Model will assist agencies in the development of their zero trust strategies and implementation plans. It also provides several ways in which CISA services can help support zero trust solutions. On the other hand, the Cloud Security Technical Reference Architecture was developed in coordination with federal government partners and is designed to guide agencies' secure migration to the cloud by explaining considerations for things like shared services and cloud security posture management.

CISA is committed to the adoption of zero trust cybersecurity principles. As organizations migrate towards zero trust architecture, their mindsets must shift from a "location-centric" to a "data-centric" approach to cybersecurity. The zero trust model can be used as a way for organizations to secure their applications and data within the enterprise, as opposed to focusing on the traditional network perimeter model as the primary means of defense.

As outlined in CISA's Zero Trust Maturity Model, data should be protected on devices, in applications, and networks, and organizations should inventory, categorize, and label data, protect data at-rest and in-transit, and deploy mechanisms for detection data exfiltration. Organizations are encouraged to begin adopting zero trust principles immediately, knowing that adopting a mature zero trust architecture can take several years. In the near term, organizations should transition from primarily storing data in on-premises data stores where they are

Question#:	17
Topic:	Secure Storage
Hearing:	America Under Siege: Preventing and Responding to Ransomware Attacks
Primary:	Senator Thom Tillis
Committee:	JUDICIARY (SENATE)

unencrypted at rest towards storing data in cloud or remote environments where they are encrypted at rest, with the ultimate goal of encrypting all data at rest.