The Department of Homeland Security's response to
Senators Carper and Johnson's December 3, 2015 Letter

1. **Since 2005, how many victims of ransomware-related crimes have reported to DHS? Does DHS track the total amount of losses reported from ransomware victims?**

   The Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center (NCCIC) has received reports of 337 ransomware-related incidents since June 2015. The NCCIC received these reports from federal government agencies, the private sector, international partners, and the general public. The Department does not track the total amount of losses caused by ransomware from these reported incidents. Data prior to June 2015 is not currently available due to recent system upgrades that did not include the incorporation of historical data.

2. **Soon after its disruption, CryptoLocker was quickly replaced by similar ransomware programs, like CryptoWall and CryptoDefense. As of December 1, 2015, how many active ransomware-type viruses is DHS tracking?**

   The NCCIC regularly works with law enforcement partners as they identify evolving ransomware variants and widely shares indicators and mitigation techniques with public and private sector partners. The categorization scheme by which the NCCIC catalogs and maintains this information does not currently allow for the calculation of the number of ransomware variants. NCCIC will review historical alerts to identify known ransomware variants. When that information is available, NCCIC will provide it to you.

3. **DHS, including the United States Computer Emergency Readiness Team (US-CERT) and the United States Secret Service, distributes cyber vulnerability and threat information to individuals, industry, and other stakeholders. Please describe any joint efforts between DHS, DOJ, and FBI to disseminate cyber threat information.**

   DHS, through the NCCIC, collaborates with the Federal Bureau of Investigation (FBI) to produce and disseminate three principal types of collaborative cyber threat information products: Alerts, Joint Indicator Bulletins, and Joint Analysis Reports:

   - Alerts (public) – provide timely information about current security issues, vulnerabilities, and exploits. Alerts are available to the public on the United States Computer Emergency Readiness Team (US-CERT) website at www.us-cert.gov.
   - Joint Indicator Bulletins (limited distribution) – provide timely notice of current cyber threats to cybersecurity stakeholders with a need-to-know.

- Joint Analysis Reports (limited distribution) – provides network defenders and cybersecurity incident responders with technical analysis of:
    - Specific tactics, techniques, and procedures describing a cybersecurity threat;
    - How to detect and identify the relevant malicious activity; and,
    - Defensive courses of action, as appropriate.

NCCIC also collaborates with law enforcement partners to effectively coordinate and respond to cybersecurity incidents. Law enforcement entities like the U.S. Secret Service (USSS) and FBI share threat indicator information with NCCIC for technical analysis. With the victim organization's approval, NCCIC then removes the victim's identifying information and shares relevant indicators of compromise with government and private sector partners for network defense purposes. These indicators are also loaded into the EINSTEIN system to directly protect federal agencies.

Examples of recent joint efforts include:

- In December 2015, NCCIC, in collaboration with the FBI, released an Alert on Dorkbot malware. Dorkbot is a botnet used to steal online payment information, participate in distributed denial-of-service (DDoS) attacks, and deliver other types of malware to victims' computers. https://www.us-cert.gov/ncas/alerts/TA15-337A
- In November 2015, NCCIC, in collaboration with the FBI, released a Joint Analysis Report (JAR-15-20151) on DDoS activity affecting financial institutions.
- In October 2015, NCCIC, in collaboration with Department of Justice (DOJ) and the FBI, released an Alert on Dridex peer-to-peer malware, which can be employed to send spam, participate in DDoS attacks, and harvest users' credentials for online services, including banking services. https://www.us-cert.gov/ncas/alerts/TA15 286A
- In July 2015, NCCIC, in collaboration with the FBI, Defense Security Service, and Defense Cyber Crime Center released a Joint Analysis Report (JAR-15-20098) on PlugX malware. This malware family, observed to be utilized by advanced persistent threat actors, has been aggressively targeting U.S. Government and industry networks.
- In March 2015, NCCIC, in collaboration with the FBI, released a Joint Indicator Bulletin (JIB-15-20040) and Cyber Information Sharing and Collaboration Program Indicator Bulletin (IB-15-10079) to alert stakeholders about groups of cyber actors that have compromised and stolen sensitive business information from U.S. Government and commercial networks through cyber espionage.
- In April 2015, NCCIC, in collaboration with the FBI, released an Alert and Joint Analysis Report (JAR-15-20061) to highlight the importance of securing end-to-end communications, which plays an important role in protecting privacy and preventing some forms of cyber attacks. https://www.us-cert.gov/ncas/alerts/TA15-120A

- In April 2015, NCCIC, in collaboration with the FBI, released an Alert on the Simda Botnet, which may allow cyber criminals to harvest user credentials, including banking information; install additional malware; or cause other malicious attacks. https://www.us-cert.gov/ncas/alerts/TA15-105A
- In April 2015, NCCIC, in collaboration with international partners and the FBI, released an Alert and a Joint Analysis Report (JAR-15-20047) on the top 30 targeted high-risk vulnerabilities exploited by cyber threat actors. https://www.us-cert.gov/ncas/alerts/TA15-119A
- In April 2015, NCCIC, in collaboration with the DOJ and FBI, released an Alert on a family of polymorphic downloaders created with the primary purpose of downloading other malware, including password stealers, rootkits, fake antivirus, and ransomware. https://www.us-cert.gov/ncas/alerts/TA15-098A
- In December 2014, NCCIC, in collaboration with the FBI, released an Alert and a Joint Indicator Bulletin (JIB-15-20055) on targeted destructive malware affecting a major entertainment company.
- In October 2014, NCCIC released an Alert on the Crypto Ransomware, including a detailed description and recommendation mitigations. https://www.us-cert.gov/ncas/alerts/TA14-295A
- In July 2014, NCCIC, in collaboration with USSS, released an Alert on Backoff point-of-sale malware, which can expose customer data such as names, mailing addresses, credit/debit card numbers, phone numbers, and e-mail addresses to criminal elements. https://www.us-cert.gov/ncas/alerts/TA14-212A
- In June 2014, NCCIC, in collaboration with DOJ and FBI, released an Alert on GameOver Zeus malware. A system infected with GameOver Zeus may be employed to send spam, participate in DDoS attacks, and harvest users' credentials for online services, including banking services. https://www.us-cert.gov/ncas/alerts/TA14-150A

4. Does DHS coordinate with the Federal Trade Commission (FTC) to educate the public about how to mitigate the threat of ransomware? If so, please describe any joint efforts with the FTC.

Yes. DHS coordinates with the Federal Trade Commission (FTC) to educate the public about a variety of cybersecurity issues, including threats and vulnerabilities like ransomware. The Department is the federal lead of the Stop.Think.Connect.™ Campaign, the national campaign that promotes safer online practices for all Americans. DHS manages an ongoing partnership of over 250 partners that include academia, non-profit organizations, and government agencies and departments. Through the Campaign, DHS and FTC coordinate to promote safer online behavior through Stop.Think.Connect.™ and the FTC's website/program OnGuard Online. For example, the FTC creates blogs posts and videos that cover multiple cybersecurity topics to Americans, including protecting oneself against phishing and ransomware. In turn, the

Department promotes their resources through various communications methods, including Stop.Think.Connect.™ Campaign's monthly partner calls, articles, blog posts, and newsletters that are sent via email to over 45,000 recipients.

5. **In testimony before the Senate Committee on Banking, Housing, and Urban Affairs last year, officials from the FBI indicated that agencies' techniques must evolve to keep pace with increasingly sophisticated botnets that can be used to disseminate viruses like ransomware. What techniques is DHS using now to combat botnets, how are those becoming less effective, and what new techniques is DHS considering to improve its ability to combat botnets in the future?**

   The NCCIC collaborates with law enforcement and industry partners to identify and "take down" botnets. These "take downs" focus on removing the central authority that controls the botnet. Relevant law enforcement actions may involve both cyber (technical blocks/mitigations) and physical (raids, seizures, arrests) actions. NCCIC conducts victim notification to U.S. Internet Service Providers and also contacts foreign CERTS to alert them to infected computers within their respective countries. For example, DHS and FBI executed two recent takedowns against the GameOver Zeus and Dridex botnets.

   To protect federal agencies against ransomware-type botnets, NCCIC leverages the EINSTEIN 3 Accelerated (E3A) system. E3A provides perimeter protection for Federal departments and agencies. E3A's two capabilities are e-mail filtering, which protects against the use of malicious file attachments and embedded links in e-mail content, and Domain Name System (DNS) sinkholing, which prevents malware already on a government computer from contacting its command and control servers.

   In regards to Botnet Trends and Solutions, there are a number of trends in the evolution of cyber threat activity (including botnets) in recent years that present challenges to NCCIC efforts:

   - Widespread use of encryption in both malware-specific communications (e.g. malware download sites and command & control) as well as general Internet traffic (e.g., webmail, news sites, blogs, etc.). Unless cyber defense technologies are designed and implemented in a way that allows them to monitor this activity, it becomes impossible to prevent and detect this activity using network-level capabilities.
     Solutions: Technology solutions already exist to address this challenge. NCCIC works with government and private sector partners to help address policy issues and privacy concerns in the implementation of the technology solutions.
   - Adversary threats "hide in the noise" of legitimate activity. Previously, specific websites or specific network traffic patterns could be uniquely tied to malware or malicious activity. However, modern threats take steps to blend in with normal user

activity, compromise and plant malware on common or legitimate websites, and embed malware communications in normal web-browsing or email traffic.
Solutions: This challenge involves both technical and policy considerations. Technology solutions exist that can improve analysts' ability to identify malicious activity hidden within "normal" user activity, but the implementation of those solutions is made more difficult by similar encryption issues and privacy concerns as identified above. Organizations should consider a balance between user convenience and the organization's responsibility to protect its systems and data.

- The volume of activity on IT networks and systems continues to grow. The Internet continues to grow, the number of devices connected to the Internet is increasing, and applications are becoming more complex and generate increasingly greater amounts of data. All of this presents a challenge in maintaining capabilities to effectively identify and block malware.
  Solutions: From the technical perspective, efforts must focus on accelerating response through automation (integrating data and traditionally manual workflows to develop new analytic tools) and scaling IT resources to enable that automation (i.e., larger capacity, faster processing). From the human resource perspective, efforts must continue to focus on recruitment, professional development/growth, and retention of a skilled cyber workforce.

6. **The disruption of CryptoLocker required coordination between DOJ, DHS, and over a dozen international law enforcement and government entities. How can this coordination be improved? Describe the impediments, if any, to further international law enforcement coordination.**

   DHS coordinates with interagency partners through their liaison officers assigned to the NCCIC and other agency cyber centers. The NCCIC's US-CERT coordinates directly with other nations' CERTs. However, federal law enforcement agencies such as USSS, U.S Immigration and Customs Enforcement (ICE), and FBI each have relevant authorities and responsibilities for cyber law enforcement according to their missions. USSS and ICE have not experienced any significant impediments to their international law enforcement coordination regarding ransomware. DHS defers to FBI regarding any further impediments to international cyber law enforcement coordination.

7. **Recent news reports suggest ransomware attackers are also targeting public safety and law enforcement agencies. Have state and local governments sought DHS's help to remove ransomware from their computers? If so, please describe the nature of any assistance sought and whether DHS was able to decrypt the computer systems.**

   NCCIC both provides and receives information through the Multi-State Information Sharing and Analysis Center (MS-ISAC) on a regular basis and recommends that state and local governments report cyber incidents through the MS-ISAC. There have not

been ramsomware incidents that have been elevated from MS-ISAC to NCCIC in 2015 nor have any State, local, tribal and territorial (SLTT) governments sought assistance directly from the NCCIC for network malware infections of ransomware. MS-ISAC does receive cyber threat indicator and mitigation information, including information on known ransomware variants from the NCCIC.

Although the MS-ISAC has not elevated any ransomware incidents to NCCIC for action, the MS-ISAC liaison to NCCIC has informed NCCIC that their associated Computer Emergency Response Team has identified and addressed 40 incidents related to ransomware associated activity on SLTT systems.

8. **Over the past 12 months, how many instances of ransomware has DHS been made aware of in federal agencies' computers? In which agencies and on what systems was the ransomware located and what was the result? Is DHS aware of instances in which federal agencies have paid ransoms to remove ransomware?**

   DHS's NCCIC has either initiated (based on EINSTEIN detection) or received 321 incident reports of ransomware-related activity specifically affecting 29 different Federal Agency networks since June 2015.

   Not all of these 321 incident reports involved actual infection with ransomware. Some incidents included reports of attempted infection, such as phishing emails intended to deliver ransomware, or ransomware that was detected and eliminated by the agency's internal security operations center. In the cases where agency systems were confirmed to be infected with ransomware, the majority of infections affected end-user workstations. In all cases, the system was removed from the network and replaced with a new, clean system with minimal impact to the user and agency.

   The Department is not aware of any instances in which federal agencies paid a malicious actor to remove ransomware from a government computer.

9. **How are DHS's EINSTEIN, ALBERT, and Enhanced Cybersecurity intrusion detection and prevention systems leveraged to reduce the instances of ransomware on computers at federal agencies, State, and local agencies, and critical infrastructure? How can that be improved?**

   DHS's EINSTEIN system has a range of capabilities that allow NCCIC to monitor, analyze, detect, diagnose, and prevent various forms of suspicious and malicious cyber activity. Ransomware is a form of malware that has a specific function, but is similar in many ways to most other forms of malware that are present in the cyber threat landscape.

The techniques that adversaries use to deliver the malware, the techniques they use to communicate with and control infected systems, the Internet infrastructure used in that command & control activity, and the low-level behavior of the malware on a victim system are all similar across most families of malware. Therefore, EINSTEIN capabilities are equally effective at detecting and blocking ransomware attack as with any other type of known malware.

ALBERT is a system owned and operated by MS-ISAC. ALBERT provides similar capabilities as EINSTEIN to detect many different families of malware, including ransomware.

DHS's Enhanced Cybersecurity Services (ECS) program is capable of preventing ransomware that uses known attack vectors. Specifically, ECS blocks outbound communications to domain names tied to ransomware activity as well as spam or phishing emails with ransomware links and attachments. ECS accomplishes this by sharing ransomware indicators with Commercial Service Providers who then "block" traffic matching those indicators from entering or exiting customer networks depending on the ECS service. ECS can only block malicious activity with indicators that it has received or was able to develop through internal analysis. Ransomware may still be able to infect ECS customers if indicators related to any given ransomware have not been shared through ECS, or if the virus enters through a method not covered by ECS' existing countermeasure services, which include DNS sinkholing, email filtering, and netflow analysis.