The Cybersecurity Information Sharing Act of 2015 (CISA) was signed into law on December 18, 2015, consisting of two major components (Karp, 2016). The first component authorizes companies to monitor and defend their information systems. The second component of CISA provides protections to private entities who voluntarily share information with the federal, state, and local governments and other private entities. These benefits include protection from liabilities, Freedom of Information Act disclosures, and non-waiver of privileges.

Under CISA, the Department of Homeland Security (DHS) National Cybersecurity and Communications Integration Center (NCCIC) shares cyber threat indicators and defensive measures with the private sector (Cybersecurity Information Sharing Act of 2015 [CISA], 2015). CISA defines cyber threat indicators as malicious reconnaissance, methods of defeating or exploiting security controls and vulnerabilities, known security vulnerabilities, malicious cyber command and control, the actual or potential harm caused by a security incident, methods for causing legitimate users to enable exploitation unknowingly, or any combination of the above. Examples of threat indicators include logs that show an IP address is testing vulnerabilities, malware found on a network, IP addresses connected to denial of service attacks, and more (Chew, Newby, & Fenwick & West LLP, 2016). Defensive measures are actions, devices, procedures, or other measures taken or applied to a system to detect, prevent or mitigate a known cyber threat or vulnerability (CISA, 2015). These measures can be firewall configurations, techniques to defend against social engineering campaigns, or anything else used to protect a network (Chew, Newby, & Fenwick & West LLP, 2016). CISA aims to help public and private entities secure their networks by sharing available information about cyber threats and defenses.

Like public entities, private parties would also share cyber threat indicators and defensive measures; however, it is required that any information transmitted is scrubbed and all personally identifiable information (PII) is removed before the data gets shared (Karp, 2016) unless it is directly related to the cyber threat. Private organizations should be required to share this information with public entities like the NCCIC to create an ideal defense strategy against cyber threats and encourage development in cybersecurity. However, mandatory information reporting could infringe upon certain rights or conflict with local or federal laws. Customers' would also worry about their private data being shared with the government. CISA provides guidance that protected health information (PHI), human resources information, consumer information, financial information, and more should be removed to ease these concerns (Karp, 2016). This guidance also encourages private entities to share an anonymized characterization of cyber threats instead of detailed information about victims. Moving forward, incentives can be added to promote the public-private partnership regarding cybersecurity. One method that could be helpful is to include grants to bring networks up to speed. Organizations would share relevant cybersecurity data and account for how grants are used to update their networks. After implementation, organizations would provide an update on how new configurations have affected their cybersecurity posture to the NCCIC.

CISA is a step forward to making a national cybersecurity defense strategy that unifies the public and private sectors. By creating the NCCIC, the government attempts to create a database on cyber threats and defense strategies that all organizations can use. Although sharing information with the NCCIC is currently voluntary, organizations will be able to secure their cybersecurity defense posture better by providing relevant information and making changes based on information others offered.

Chew, H., Newby, T. G., & Fenwick & West LLP. (2016, October 24). *The Cybersecurity Information Sharing Act of 2015: An Overview*. Retrieved from Lexology: https://www.lexology.com/library/detail.aspx?g=31bc698a-ec4d-4b9b-a8a9-46d893777a10

Cybersecurity Act of 2015. (H.R. 2029-694). *2015*. Retrieved from https://www.cisa.gov/sites/default/files/publications/Cybersecurity%20Information%20Sharing%20Act%20of%202015.pdf

Karp, B. S. (2016, March 3). *Federal Guidance on the Cybersecurity Information Sharing Act of 2015*. Retrieved from Harvard Law School Forum on Corporate Governance: https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/