Appendix 1 – Comparison of Several of Zoom's WISP and SHIELD Act Provisions

Program Elements	Zoom's WISP	SHIELD Data Security Program
Administrative Safeguards	Designate a Head of Security, who reports to the CEO quarterly and to the BOD semi-annually	Not Required
	Designate one or more employees to coordinate and be accountable for the WISP; Report directly to the Head of Security	Designate one or more employees to coordinate the data security program
	Identify material internal and external risks to the security, confidentiality, and integrity of personal information that could result in: unauthorized disclosure; misuse; loss; alteration; destruction; or compromise of such information	Identify reasonably foreseeable internal and external risks
	Assess the sufficiency of any safeguards in place to control these [material internal and external] risks	Assess the sufficiency of safeguards in place to control the identified risks
	Not Discussed	Train and manage employees in the security program's practices and procedures
	Not Discussed	Select service providers capable of maintaining appropriate safeguards, and requires those safeguards by contract
	Evaluation and adjustment of the WISP in light of the results of the testing or monitoring required by these terms	Adjust the security program in light of business changes or new circumstances
	Zoom's WISP	**SHIELD Data Security Program**
	Continue to operate a vulnerability management program to address known vulnerabilities, and have reasonable safeguards to discover and fix new vulnerabilities	Assess the risks in network and software design
	Employ reasonable encryption and security protocols, including by encrypting all personal information at rest and in transit except where the user	Assess the risks in information processing, transmission and storage

Technical Safeguards	fails to utilize a Zoom app or Zoom software for the transmission. Zoom will update and upgrade its security and encryption as industry standards evolve	
	Design and implement security code review processes to identify and remediate common security vulnerabilities	Detect, prevent and respond to attacks or system failures
	Design and implement regular testing or monitoring of the effectiveness of the safeguards' key controls, systems, and procedures	Regularly test and monitor the effectiveness of key controls, systems and procedures
Physical Safeguards	**Zoom's WISP**	**SHIELD Data Security Program**
	Not Discussed	Assess the risks of information storage and disposal
	Not Discussed	Detects, prevent and respond to intrusions
	Not Discussed	Protect against unauthorized access to or use of private information during or after the collection, transportation and destruction or disposal of the information
	Not Discussed	Dispose of private information within a reasonable amount of time after it is no longer needed for business purposes by erasing electronic media so that the data cannot be read or reconstructed