CIS Control	CIS Safeguard	Asset Type	Security Function	Title	Description	IG1	IG2	IG3
1				Inventory and Control of Enterprise Assets	*Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also support identifying unauthorized and unmanaged assets to remove or remediate.*	x	x	x
2				Inventory and Control of Software Assets	*Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.*	x	x	x
3				Data Protection	*Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.*	x	x	x
4				Secure Configuration of Enterprise Assets and Software	*Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).*	x	x	x
5				Account Management	*Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.*	x	x	x
6				Access Control Management	*Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.*	x	x	x
7				Continuous Vulnerability Management	*Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.*	x	x	x
8				Audit Log Management	*Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.*	x	x	x
9				Email and Web Browser Protections	*Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.*	x	x	x
10				Malware Defenses	*Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.*	x	x	x
11				Data Recovery	*Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.*	x	x	x
12				Network Infrastructure Management	*Establish, implement, and actively manage (track, report, correct) network devices, in order to prevent attackers from exploiting vulnerable network services and access points.*	x	x	x
13				Network Monitoring and Defense	*Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.*	x	x	x
14				Security Awareness and Skills Training	*Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.*	x	x	x
15				Service Provider Management	*Develop a process to evaluate service providers who hold sensitive data, or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.*	x	x	x
16				Application Software Security	*Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.*	x	x	x
17				Incident Response Management	*Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.*	x	x	x
18				Penetration Testing	*Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology), and simulating the objectives and actions of an attacker.*	x	x	x