NIST SP 800-171

THE 14 INFORMATION SECURITY CONTROL FAMILIES AFFECTED BY NIST SP 800-171:

Access Control	Who is authorized to view CUI data?
Awareness and Training	Are people properly trained info?to manage, store and process CUI?
Audit and Accountability	Are records kept of authorized and unauthorized access? Can violators be identified?
Configuration Management	How are your networks and protocols information systems designed and documented?
Identification and Authentication	Are users who they say they are? Is the user accessing CUI real or an imposter?
Incident Response	What happens if a breach or security threat occurs, including proper notification?
Maintenance	What program is in place for information system maintenance, and who owns that responsibility?
Media Protection	How are electronic and hard copy records and backups stored, and who has access?
Physical Protection	Who has physical access to your systems, equipment, and storage environments?
Personnel Security	How are employees screened prior to gaining access to CUI?
Risk Assessment	What is the risk that CUI will be compromised? Risk equals the likelihood that security controls "don't" work as designed and the resulting impact to the organization.
Security Assessment	Are security controls implemented correctly, operating as intended and producing the desired outcome?
System and Communications Protection	Are information system protection controls working properly?
System and Information Integrity	How quickly are threats detected, identified and remediated?

FIND OUT MORE AT

www.cyberdefenses.com/nist-sp-800-171/

CYBERDEFENSES

1 Chisholm Trail, Suite 327. Round Rock TX 78681

512-255-3700 / info@cyberdefenses.com / www.cyberdefenses.com