	Espionage Cases	Sabotage Cases
Technical action and indicators	Access of Information outside of need to know	Creation of backdoor account
	Concealment strategies	Download and installation of malicious code and tools (e.g., password cracker or virus)
	Download and installation of malicious code and tools	Failure to comply with configuration management policy
	Hacking	Unauthorized information transfer
	Unauthorized encryption of information	Access from new employer' s system
	Unauthorized information transfer	Installation of unauthorized modem (hardware backdoor) for later access
	Violation of acceptable use policy	Disabling of anti-virus on insider' s computer to test virus for later use in sabotage
	Violation of password management policy	Network probing
Harmful Technical Actions	Printing documents	Denial of service by changing passwords or disabling access
	Copying information to disks	Deletion of files, databases, or systems - including system history files
	Relabeling of disks	Constructing, downloading, testing, or planting log ic bombs
		Stealing or sabotaging backups
		Terminating programs or shutting down computers or equipment
		Cutting cables
		Reformatting disks
		Downloading a virus onto

		customers' computers
		Turning off system logging
		Web site defacement
		Use of organization's system following termination to send derogatory email to customers
		Modification of ISP's system logs to frame someone else for actions
		Accessing confidential information and making it av ailable to customers, employees, or the public
		Theft of hardware, software, and documentation
Technical Rule Violations	Violation of need to know	Downloading and use of "hacker tools" such as rootkits, password sniffers, or password crackers
	Violation of SCIF physical security policies and pr ocedures	Failure to create backups as required
	Download and use of password cracker	Failure to document systems or software as required
	Unauthorized encryption of information	Unauthorized access of customers' systems
	Compromise of supervisor's computer	Unauthorized use of coworkers machines left logged in
	Unauthorized "web surfing" and watching videos on office computer in violation of acceptable use policy	Sharing passwords with others
		System access following termination

		Refusal to swipe badge to record physical access
		Access of web sites prohibited by acceptable use policy
		Refusal to return laptop upon termination
		Use of backdoor accounts
		Use of organization’s system for game playing, violating acceptable use policy