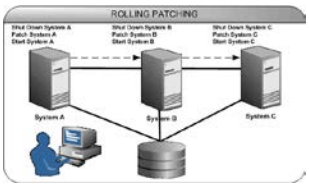
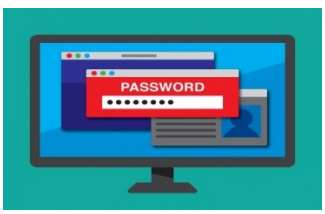
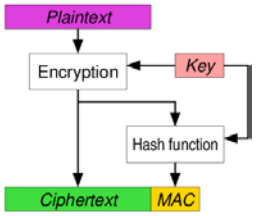
Quick Start Guide to CyberSecurity Recommendations and Tips

	Be the leader when it comes to CyberSecurity. Make it a priority and hold everyone accountable.
	Identify those responsible and determine capabilities, timelines, job descriptions, and funding. Look to other government agencies/private contractors to augment existing resources.
	Communicate often regarding the need to remain vigilant in an ever changing CyberSecurity landscape. Establish and/or annually review data security policies and procedures.
	Establish a yearly judge/employee training program regarding CyberSecurity.
	Prepare a CyberSecurity action plan. Test at least yearly. The plan at a minimum should have a chain of command, recommended action steps, a communication component, and other government (vendors) identified with contact information.
	Ensure that system firewall settings are configured and adapted to keep your systems secure. Review email security settings filtering malicious emails/attachments.
	Have a software patch schedule for servers, storage, software, desktops, and hardware. Backup systems on a very frequent basis and have an off-site storage process.
	Enhance password complexity and length (recommendation is 15 characters with complexity), recommend changing every six (6) months. Recommend screen lockouts at 15-30 minutes.

Bryant Baehr, Oregon Judicial Department_2017

	Encrypt mobile devices. Encryption is the only way to ensure (as best as possible) that a stolen mobile device is not a risk to the court.
	Run anti-virus scans on all desktop, laptops, and servers. Ensure that anti-virus software is updated on a regular basis.
	Plan an external system penetration test. Yearly is recommended. Prepare an action plan once the results of the penetration test are known.
	Secure your wireless network. Do you offer "free or guest" Wi-Fi? If so, ensure that the "free or guest" Wi-Fi is segregated from your production systems and/or at a minimum capped at a certain speed to prevent production disruptions.
	Be prepared to invest time and resources in technology staff training (on-site, video, and off-site) to keep up with CyberSecurity trends and preventative actions that can be taken.
	CyberSecurity will slow you down a bit – plan on it. Ransomware, successful malicious email attacks, and systems that are compromised are generally preventable.