Summary of CCA's Critical Security Controls

Condensed from TripWire's "The Executive's Guide to the Top 20 Critical Security Controls"

1. Inventory of Authorized & Unauthorized Devices
Reduce the ability of attackers to find & exploit unauthorized & unprotected systems: use active monitoring & configuration management to maintain an up-to-date inventory of devices connected to the enterprise network, including servers, workstations, laptops, and remote devices.

2. Inventory of Authorized & Unauthorized Software
Identify vulnerable or malicious software to mitigate or root out attacks: devise a list of authorized software for each type of system & deploy tools to track software installed (including type, version, and patches) & monitor for unauthorized or unnecessary software.

3. Secure Hardware/Software Configurations on Mobile Devices, Laptops, Workstations & Servers
Prevent attackers from exploiting services & settings that allow easy access via networks and browsers: Build a secure image that is used for all new systems deployed to the enterprise, host these standard images on secure storage servers, regularly validate and update these configurations, and track system images in a configuration management system.

4. Continuous Vulnerability Assessment & Remediation
Proactively identify and repair software vulnerabilities reported by security researchers or vendors: Regularly run automated vulnerability scanning tools against all systems and quickly remediate any vulnerabilities, with critical problems fixed within 48 hours.

5. Malware Defenses
Block malicious code from tampering with system settings or contents, capturing sensitive data, or spreading: Use automated anti-virus and anti-spyware software to continuously monitor and protect workstations, servers, and mobile devices. Automatically update such anti-malware tools on all machines on a daily basis. Prevent network devices from using auto-run programs to access removable media

6. Application Software Security
Neutralize vulnerabilities in web-based and other application software: Carefully test internally developed & 3rd-party application software for security flaws including coding errors & malware. Deploy web app firewalls that inspect all traffic & explicitly check for errors in all user input (including by size & data type).

7. Wireless Device Control
Protect the security perimeter against unauthorized wireless access: Allow wireless devices to connect to the network only if they match an authorized configuration and security profile and have a documented owner and defined business need. Ensure that all wireless access points are manageable using enterprise management tools. Configure scanning tools to detect wireless access points

8. Data Recovery Capability
Minimize the damage from an attack: Implement a trustworthy plan for removing all traces of an attack. Automatically back up all information required to fully restore each system, including the operating system, application software, and data. Back up all systems at least weekly; back up sensitive systems more often. Regularly test the restoration process.

9. Security Skills Assessment & Appropriate Training to Fill Gaps
Find knowledge gaps, and fill them with exercises and training: Develop a security skills assessment program, map training against the skills required for each job, and use the results to allocate resources effectively to improve security practices.

10. Secure Network Device Configurations- Firewalls, Routers & Switches
Preclude electronic holes from forming at connection points with the Internet, other organizations, and internal network segments: Compare firewall, router, and switch configurations against standards for each

type of network device. Ensure that any deviations from the standard configurations are documented and approved and that any temporary deviations are undone when the business need abates

11. Limitation and Control of Network Ports, Protocols & Services
Allow remote access only to legitimate users and services: Apply host-based firewalls and port-filtering and -scanning tools to block traffic that is not explicitly allowed. Properly configure web servers, mail servers, file and print services, and domain name system (DNS) servers to limit remote access. Disable automatic installation of unnecessary software components. Move servers inside the firewall unless remote access is required for business purposes.

12. Controlled Use of Administrative Privileges
Protect and validate administrative accounts on desktops, laptops, and servers to prevent two common types of attack: (1) enticing users to open a malicious e-mail, attachment, or file, or to visit a malicious website; and (2) cracking an administrative password and thereby gaining access to a target machine. Use robust passwords that follow Federal Desktop Core Configuration (FDCC) standards.

13. Boundary Defense
Control the flow of traffic through network borders, and police content by looking for attacks and evidence of compromised machines: Establish multi-layered boundary defenses by relying on firewalls, proxies, demilitarized zone (DMZ) perimeter networks, and other network-based tools. Filter inbound and outbound traffic, including through business partner networks ("extranets").

14. Maintenance, Monitoring & Analysis of Audit Logs
Use detailed logs to identify and uncover the details of an attack, including the location, malicious software deployed, and activity on victim machines: Generate standardized logs for each hardware device and the software installed on it, including date, time stamp, source addresses, destination addresses, and other information about each packet and/or transaction. Store logs on dedicated servers, and run biweekly reports to identify and document anomalies.

15. Controlled Access Based on the Need to Know
Prevent attackers from gaining access to highly sensitive data: Carefully identify and separate critical data from information that is readily available to internal network users. Establish a multilevel data classification scheme based on the impact of any data exposure, and ensure that only authenticated users have access to non-public data and files.

16. Account Monitoring & Control
Keep attackers from impersonating legitimate users: Review all system accounts and disable any that are not associated with a business process and owner. Immediately revoke system access for terminated employees or contractors. Disable dormant accounts and encrypt and isolate any files associated with such accounts. Use robust passwords that conform to FDCC standards.

17. Data Loss Prevention
Stop unauthorized transfer of sensitive data through network attacks and physical theft: Scrutinize the movement of data across network boundaries, both electronically and physically, to minimize the exposure to attackers. Monitor people, processes & systems using a centralized management framework.

18. Incident Response & Management
Protect the organization's reputation, as well as its information: Develop an incident response plan with clearly delineated roles & responsibilities for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence & restoring the integrity of the network and systems.

19. Secure Network Engineering
Keep poor network design from enabling attackers: Use a robust, secure network engineering process to prevent security controls from circumvention. Deploy a network architecture with at least three tiers: DMZ, middleware, private network. Allow rapid deployment of new access controls to quickly deflect attacks

20. Penetration Tests & Red Team Exercises

Use simulated attacks to improve organizational readiness: conduct regular internal & external pen tests that mimic an attack to identify vulnerabilities & gauge potential damage. Use periodic red team exercises: all-out efforts to access critical data & systems & test existing defenses & response capabilities