Minimum Security Standards

TAC – DECEMBER 4, 2015

RICHARD BLAIR

Introduction

- Cybersecurity now on the radar of court business leadership
- Karl requested draft of "Minimum Set of Security Standards"
- Discuss and ratify by TAC
- Recommend to COT and AJC for formal adoption

Today's goal: present the foundation for further discussions

Computer Room & Environmental Controls

- All servers and network equipment should be secured from general access
- Unauthorized personal are escorted while in the controlled access areas
- Where applicable, UPS as well as smoke, fire, water, and temperature detection devices should be in place

User Authentication & Access Control

- User access to computer and network resources are only granted by management of the requester
- User IDs conform to a standard format and generic User IDs are only used for service accounts/programmatic access.
- User IDs are deactivated for inactivity then deleted after prolonged inactivity
- Password management (length, format, security, expiration)

AJIN Access from Outside the Domain

- Direct access to the AJIN network from outside sources must come through approved AOC methods: no backdoors
- User access is through VPN managed by AOC Network Services
- Programmatic access to AJIN network is through AOC-approved technologies

Computing and Network Devices within AJIN

- Standards governing PC desktops residing on AJIN – anti-virus, scanning, screen savers, and third-party software security
- Standards governing servers residing on AJIN – anti-virus, scanning, access logging, patch management/security vulnerabilities
- Employee termination and system security
- Network monitoring and data capturing tools