The CIP standards and requirements have many dates and activities necessary for compliance. There are A LOT of recurring tasks that can easily slip through the cracks. Below is an outline of timing for performing against various CIP standards.

### CIP COMPLIANCE PROCESS MANAGEMENT

#### AS NEEDED
- CIP-003: Update to CIP Senior Manager and Delegations
- CIP-004: Granting/Removal Physical and/or Cyber Access
- CIP-006: Visitor Escort and Logging into PSP
- CIP-007: Patch Install or Mitigation Plan Development/Update
- CIP-007: Malicious Code Signature Update
- CIP-008: Incident Response and Update to Incident Response Plan
- CIP-009: Lessons Learned & Plan Updates
- CIP-010: Baseline Updates and Documentation

#### ONGOING
- CIP-006: Monitor and Response to Unauthorized access into PSP
- CIP-006: Monitoring and Alarming of Unauthorized Access to PACS
- CIP-006: PSP Activity Logging and Log Retention
- CIP-007: System Logging, Alerting, and Log Retention

### 15 CALENDAR DAYS
- CIP-007: Sample Log Review

### 35 CALENDAR DAYS
- CIP-007: Patch Evaluation
- CIP-010: Baseline Review

### CALENDAR QUARTER
- CIP-004: Security Awareness Reinforcement
- CIP-004: Verify Individuals with Active Electronic Access or Unescorted Physical Access

### 15 CALENDAR MONTHS
- CIP-002: BES Cyber System Identification
- CIP-003: CIP Senior Manager Approval of Policies
- CIP-004: Verify Access to BES Cyber System Information
- CIP-004: Verify Access Privileges
- CIP-004: Cyber Security Training
- CIP-004: Cyber Security Awareness Reinforcement
- CIP-007: Password Change
- CIP-008: Incident Response Plan Test
- CIP-009: Test Sample of Recovery Information
- CIP-009: Recovery Plan Test for High & Medium
- CIP-010: Paper or Active VA

### 24 CALENDAR MONTHS
- CIP-006: Maintenance and Testing of PACS

### 36 CALENDAR MONTHS
- CIP-003: Incident Response Plan Test
- CIP-009: Recovery Plan Test for High Impact
- CIP-010: Active VA for High Impact

### 7 YEARS
- CIP-004: Personnel Risk Assessment

http://www.sans.org/icc456