**Pre-Approved Actions (PAA)**

**Purpose**

Before beginning a mission, the IR Team should discuss pre-approved actions, such was blocking ports

and services or conducting scanning etc. with the Mission and Network owners to understand

the on-network boundaries. The PAA should specify which actions the IR Team is able to make and what

approval or reporting is required.

**Pre-Approved Actions**

In order to defend identified critical resources, the following Pre-Approved Actions are authorized by

the Mission Owner (MO):

1. Task: Identify
   1. Enumerated network and established a configuration management baseline
   2. Threat assessment, OPE to operators
   3. Identified CVEs for systems
   4. Updated network maps and documentation
   5. Implement team-provided network defense tools and sensors (SecOnion/Wazuh/Wireshark/etc)
   6. Conduct baseline scanning of all non-ICS enclaves (incl: devices & traffic flows)  
      Block unnecessary ports & services not required for device to perform its intended function
   7. Perform risk assessment
2. Task: Protect
   1. Ensure placement of sensors
   2. Monitoring logs and aggregation
   3. Improved security posture of systems based on risk/threat assessment
   4. Prioritized hardening approach to x high-risk CVEs per STIG, SP 800-53
3. Task: Detect
   1. Detected and captured artifacts
   2. Quick network forensics to confirm suspicious traffic
   3. Monitor team hands-off events to Pursuit team for deep-dives
   4. Report of events
4. Task: Respond
   1. Focused Incident handling and change control
   2. Conduct forensics
   3. Maintain monitoring
   4. Change requests for Protect recommendations
   5. Also react to new CVE, CERT reports and INTSUM
5. Task: Recover
   1. Document (Roll up) change management
   2. Provide threat analysis
   3. Provide recommendations for additional follow-on security measures
   4. Report to Mission Owner, Intel Sharing and Higher Authority

Printed Business Owner name

Signature\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_