Critical Infrastructure Threat Response Checklist

1. Immediate Actions

- Identify and confirm the nature of the threat.
- Notify response team and key stakeholders.
- Record date, time, and method of threat detection.
- Ensure personal safety and secure the site if necessary.
- Activate incident response plan.

2. Containment & Assessment

- Isolate affected systems or areas to prevent escalation.
- Assess impact to critical operations and infrastructure.
- Document all containment steps taken.
- Coordinate with internal/external security teams.

3. Communication

- Inform leadership and regulatory authorities as required.
- Provide situation updates to staff and partners.
- Log all communications (date, time, recipient, content).

4. Investigation

- Collect relevant data, logs, and evidence.
- Interview witnesses or personnel involved.
- Determine possible source and scope of threat.
- Document findings and create incident timeline.

5. Mitigation & Recovery

- Implement mitigation procedures to neutralize the threat.
- Restore affected services and utilities step-by-step.
- Test and confirm system stability post-recovery.
- Maintain detailed records of actions taken.

6. Post-Incident Actions

- Conduct debrief and after-action review.
- Update incident documentation and lessons learned.
- Revise and improve response plans based on findings.
- Report to external agencies or regulators if required.

7. Contacts & Resources

Role/Organization	Name/Contact	Phone/Email
Incident Response Lead		
Facilities Security		
IT Support		
Law Enforcement		

Note: *Store this checklist in an accessible location. Update it regularly as organizational needs change.*