ADVISORY: PREPAREDNESS FOR CIVIL DEFENSE MOCK DRILLS AND CYBER SECURITY MEASURES

Advisory Team
OPSEC Labs Pvt Ltd
May 6, 2025

EXECUTIVE SUMMARY

In response to the Ministry of Home Affairs (MHA) directive for nationwide civil defence mock drills on May 7, 2025, across 244 designated districts, we at **OPSEC Labs,** are issuing this comprehensive advisory to help organizations prepare effectively. These drills-the first of such scale since 1971-come amid escalating tensions between India and Pakistan following the April 22 Pahalgam terror attack. This advisory provides actionable guidance for security managers, CISOs, crisis coordinators, and business owners to ensure organizational readiness.

BACKGROUND AND CONTEXT

The Government of India, through the Ministry of Home Affairs (MHA), has mandated nationwide civil defense mock drills from May 7–9, 2025, across 244 districts, including Bengaluru, in response to heightened tensions with Pakistan following the Pahalgam terror attack on April 22, 2025. These drills, guided by the Civil Defence Rules, 1968, aim to prepare organizations and civilians for potential hostile scenarios, such as aerial attacks or missile strikes. Concurrently, the Indian Computer Emergency Response Team (CERT-In) has reported a surge in cyber threats, including web defacements and data theft targeting Indian businesses, particularly in IT hubs like Bengaluru.

The MHA has ordered these nationwide civil defence exercises to assess and enhance preparedness in the event of a hostile attack. The drills will include air raid warning sirens, blackout simulations, evacuation rehearsals, and testing of emergency response systems. Key activities will include training civilians on self-protection measures, implementing crash blackout protocols, camouflaging vital installations, and updating evacuation plans.

KEY ADVISORY GUIDELINES

PHYSICAL SECURITY PREPAREDNESS

1. **Familiarize yourself with local building safety and emergency guidelines**
   - Review building evacuation plans and assembly points
   - Identify emergency exits, stairwells, and safe zones
   - Ensure **emergency lighting systems** are functional

2. **Review state and local emergency management guidelines**
   - Access your **state disaster management authority's website** for specific guidelines
   - Check district-**level civil defence procedures** applicable to your area

3. **Be aware of proximity to sensitive locations**
   - Map **nearby government or military establishments** that could be potential targets
   - Understand how their security protocols **might affect your operations** during heightened alerts

4. **Enhance situational awareness**
   - Brief **security personnel to remain vigilant** for suspicious activities
   - Implement additional access control measures if necessary

5. **Prepare for potential service disruptions**
   - **Have contingency plans for internet and telecommunications** outages
   - Prepare for possible **transportation disruptions** or restrictions
   - Stock essential supplies including water, non-perishable food, and medical supplies

6. **Prepare for Air Raid Sirens and Warnings**
   - Educate employees on recognizing air raid sirens, which will be tested during the drills.
   - Practice **drop-and-cover** techniques and identify sturdy shelters within your premises.

  - Ensure clear communication channels to relay warnings to all staff during the drills.

7. **Develop evacuation planning**
   - Create or update **evacuation procedures** aligned with civil defence guidelines
   - Designate and train **evacuation wardens** for each floor/department

8. **Budget for safety equipment and training**
   - Invest in **emergency communication devices**
   - Ensure first aid kits, flashlights, and emergency supplies are adequately stocked

9. **Prepare for potential internet blackouts or disruptions**
   - Maintaining offline backups of critical data.
   - Establishing alternative communication channels, such as satellite phones or radios.

10. **Anticipate transport blackouts**
    - Arranging flexible work-from-home options.
    - Identifying alternative routes for essential travel.

11. **Coordinate with neighbouring businesses**
    - Establish mutual aid agreements with nearby organizations
    - Share emergency contact information and resources
    - Develop coordinated response procedures

CYBERSECURITY MEASURES

9. **Strengthen cyber defences**
   - Implement heightened **monitoring for network intrusions**
   - Update all security patches and **conduct vulnerability assessments**
   - Enable **multi-factor authentication** for critical systems

10. **Prepare for website protection**
    - Heighten defences against **web defacements**, which are increasingly targeting Indian businesses.
    - Implement DDoS protection measures

- **Backup** website data and prepare restoration protocols

11. **Protect critical data**
    - Encrypt sensitive information
    - Consider air-gapping critical systems during high-alert periods

12. **Monitor for misinformation**
    - Establish **protocols** to verify information before sharing internally or externally
    - Be alert to **deepfakes** and manipulated media that might cause panic
    - Designate **authorized spokespersons** for organizational communications

COMMUNICATION PROTOCOLS

13. **Update emergency contact lists**
    - Compile and distribute contact details for Internal emergency team, Local authorities, Emergency services, Key vendors and partners

14. **Establish communication redundancies**
    - Prepare **alternate communication channels** if primary systems fail
    - Develop a communication tree for rapid information dissemination

15. **Cooperate with authorities**
    - Maintain open channels with building management and security personnel
    - Be responsive to **additional security measures** implemented in your facility
    - Follow instructions from **civil defence authorities** during drills

16. **Stay informed through official channels**
    - **Monitor** notifications from district authorities
    - **Subscribe** to emergency alert systems
    - Avoid **spreading unverified information**

EXERCISING OPSEC (OPERATIONAL SECURITY)

- Do not **capture** or share photos or videos of **troop or police movements.**
- Do not discuss **sensitive operational details** in public or on social media.
- Share confidential information only with authorized personnel on a need-to-know basis.
- Report any suspicious requests for information to your security team immediately.

DURING THE MOCK DRILL (MAY 7)

17. **Recognize and respond to warning sirens**
    - Familiarize staff with **air raid warning** signals
    - Train appropriate responses when sirens are activated
    - Conduct briefings prior to May 7 on expected scenarios

18. **Participate constructively in blackout procedures**
    - Follow any instructions for crash blackouts during the drill
    - Test backup power systems if available
    - Use the opportunity to identify lighting vulnerabilities

19. **Maintain calm and discourage panic**
    - Brief employees that this is a preparedness exercise
    - Discourage spreading of rumours or unverified information
    - Emphasize that participation improves overall safety

POST-DRILL ACTIONS

20. **Document lessons learned**
    - Conduct a debrief session following the drill
    - Identify gaps in response or communication

21. **Review and enhance business continuity plans**
    - Use insights from the drill to strengthen continuity planning
    - Assess supply chain vulnerabilities
    - Consider geo-redundancy for critical operations

SPECIAL CONSIDERATIONS FOR BENGALURU-BASED ORGANIZATIONS

As Bengaluru is among the 244 districts designated for these exercises, local organizations should:

- Monitor communications from Karnataka State Disaster Management Authority
- Prepare for possible IT infrastructure testing given the city's technology hub status
- Coordinate with tech park or business complex management regarding drill participation.

KEY RESOURCES

- Ministry of Home Affairs: **mha.gov.in**
- Karnataka State Disaster Management Authority: **ksdma.karnataka.gov.in**
- CERT-In: **cert-in.org.in**
- NCIIPC: **nciipc.gov.in**
- MyGov Portal: **mygov.in**
- Press Information Bureau: **pib.gov.in**
- Emergency Helpline: 100, 112

For further assistance, contact our team at advisory@opsec.in. OPSEC Labs is committed to ensuring your organization's readiness for the cyber defense drills and ongoing security challenges in Bengaluru and beyond.

This advisory is based on publicly available information as of May 6, 2025, and may be updated as additional official guidance becomes available.

Stay vigilant, stay prepared, and stay safe.

Advisory Team,
OPSEC Labs Pvt Ltd
https://opsec.in | advisory@opsec.in