OPORD 3: OPERATION SUPPLY CHAIN SENTINEL

CLASSIFICATION: UNCLASSIFIED//FOR TRAINING USE ONLY
EXERCISE OPORD 003-25
FROM: Cyber Supply Chain Defense Task Force
DTG: 171000ZJUL25

1. SITUATION

a. Enemy Forces: EXERCISE - Sophisticated threat group "Shadow Vendor" with supply chain compromise capabilities. Known for patience and advanced evasion techniques.

b. Friendly Forces: Task force of 75 personnel including government cyber specialists and industry security teams from major defense contractors.

c. Environment: EXERCISE - Discovery of simulated compromise in widely-used software affecting multiple defense contractors.

2. MISSION

Cyber Supply Chain Defense Task Force conducts emergency response operations from 171400Z to 201400Z JUL 25 to identify, isolate, and remediate simulated supply chain compromises affecting defense industrial base networks in order to restore secure operations and prevent further infiltration during EXERCISE.

3. EXECUTION

a. Concept of Operations: Rapid assessment, containment, and remediation across affected contractor networks with coordinated government support.

b. Tasks to Subordinate Units:

- **Assessment Team:** Conduct rapid security assessments at affected contractor facilities within 24 hours.
- **Isolation Team:** Implement network segmentation and containment measures to prevent lateral movement.
- **Remediation Team:** Clean compromised systems and restore secure configurations.
- **Intelligence Team:** Analyze threat actor TTPs and develop countermeasures.

c. Fires: Not applicable.

d. Coordinating Instructions:

- Maintain contractor proprietary information security

- Coordinate with FBI for threat attribution (EXERCISE)
- Provide regular updates to senior leadership

4. SERVICE SUPPORT

a. Logistics: Rapid deployment teams equipped with mobile cyber analysis equipment.

b. Transportation: Government vehicles available for team deployment to contractor locations.

c. Maintenance: Technical support teams available 24/7 for equipment issues.

5. COMMAND AND SIGNAL

a. Command: Task force commander maintains operational control. Industry partners retain administrative control of their personnel.

b. Signal: Secure government communications for coordination. Industry-specific channels for internal communications per EXERCISE protocols.

SUCCESS CRITERIA: All compromised systems identified and cleaned within 72 hours