



# Security Advisory System

TBL/Field Services (March 2003)

*Note: Should the threat condition escalate to Orange or Red, an immediate assessment of the nature of the threat (type and location) will be made and BPA's response will be gauged accordingly. The requirements below may be adjusted according to the nature of the threat warning.*

<p><b>CONDITION RED</b></p> <p><b>SEVERE</b> &gt;</p> <p>Severe Risk of Terrorist Attacks</p>	<p><b>Continue to implement ALL standards in condition ORANGE and:</b></p> <p><i>Physical:</i></p> <ul style="list-style-type: none"> <li>• Be prepared to evacuate facilities on short notice</li> <li>• Crews on telephone standby if evacuated</li> <li>• Utilize the Regional telephone tree for updated information</li> <li>• Local authorities, private security, or National Guard may secure facility based on the nature of the threat</li> <li>• If no direct threat against BPA exists, BPA may elect to operate under ORANGE/HIGH conditions</li> </ul>	<p><i>Cyber:</i></p> <ul style="list-style-type: none"> <li>• Internet use is restricted to specifically approved activities</li> <li>• Emergency Response Teams may be activated</li> <li>• Internet access may be terminated at any time</li> <li>• Vulnerable services may be terminated without notice</li> <li>• Continuous monitoring of internet activity and Network Intrusion Detection Systems is in effect</li> <li>• Exercise extreme caution regarding e-mail and attachments</li> </ul>
<p><b>CONDITION ORANGE</b></p> <p><b>HIGH</b> &gt;</p> <p>High Risk of Terrorist Attacks</p>	<p><b>Continue to implement ALL standards in condition YELLOW and:</b></p> <p><i>Physical:</i></p> <ul style="list-style-type: none"> <li>• Public access prohibited</li> <li>• Restoration of critical grid facilities ASAP</li> <li>• All tools and equipment ready and available</li> <li>• Conduct perimeter observation patrols</li> </ul>	<p><i>Cyber:</i></p> <ul style="list-style-type: none"> <li>• Internet use is restricted to "Essential Business Use" only</li> <li>• All internet access will be monitored</li> <li>• Do not open e-mails or e-mail attachments from unknown or suspect sources</li> </ul>
<p><b>CONDITION YELLOW</b></p> <p><b>ELEVATED</b> &gt;</p> <p>Significant Risk of Terrorist Attacks</p>	<p><b>Continue to implement ALL standards in condition GREEN / BLUE and:</b></p> <p><i>Physical:</i></p> <ul style="list-style-type: none"> <li>• Increased vigilance and personal safety awareness</li> <li>• Call Dispatch upon arrival at site</li> <li>• Use "buddy system" to secure and lock gates and doors except while passing through</li> <li>• Obtain private security or law enforcement assistance for site security</li> <li>• Screen visitors, restrict access</li> <li>• Secure vehicles in an enclosed area</li> <li>• No access to energized yards unless necessary for maintenance or construction</li> <li>• Move vehicles, trash containers, etc., 30 yards from buildings</li> <li>• Be alert for suspicious or improvised explosive devices</li> </ul>	<p><i>Cyber:</i></p> <ul style="list-style-type: none"> <li>• Internet use is restricted to Official Business Use only</li> <li>• Site blocking and Email blocking, and special network configurations may be implemented</li> <li>• Do not open Email from unknown sources and be wary of unusual Email from known sources</li> <li>• Report all suspicious network activity to Cyber Security</li> </ul>
<p><b>CONDITION BLUE</b></p> <p><b>GUARDED</b> &gt;</p> <p>General Risk of Terrorist Attacks</p>	<p><i>Physical:</i>      <i>Security &amp; Emergency Management phone number (503) 230-3779</i></p> <ul style="list-style-type: none"> <li>• Review emergency evacuation and recall plans</li> <li>• Form contracts for private security or local law enforcement support</li> <li>• Exercise Operational Security procedures</li> <li>• Review bomb threat and suspicious mail procedures</li> <li>• Perform visual inspections of exterior areas</li> <li>• Turn on yard and building lights</li> </ul>	<p><i>Cyber:</i>      <i>Cyber Security phone number (503) 230-5088</i></p> <ul style="list-style-type: none"> <li>• All normal BPA Cyber use policies apply under Condition Green</li> <li>• Employees may not access private, non-BPA e-mail accounts through BPA internet connections under any conditions</li> <li>• Normal virus response processes will be followed</li> <li>• Exercise additional care regarding e-mail, e-mail attachments and web browsing</li> </ul>
<p><b>CONDITION GREEN</b></p> <p><b>LOW</b> &gt;</p> <p>Low Risk of Terrorist Attacks</p>	<ul style="list-style-type: none"> <li>• Screen incoming mail for suspicious items</li> <li>• Stage concrete vehicle barriers in storage areas for later use, if necessary</li> <li>• Develop sources for local security services</li> <li>• Develop emergency supplies of food, water, etc.</li> <li>• Establish contact and rapport with local emergency services providers (begin minimum security standards)</li> </ul>	<ul style="list-style-type: none"> <li>• Internet controls may be increased at Condition Blue</li> <li>• Personal and non-business use are allowed but may become restricted at Condition Blue</li> <li>• Report all suspicious network activity to Cyber Security</li> </ul>