Multi-State ISAC
Procedures and Protocols for Cyber Alert Indicator
Adopted by the MS-ISAC October 31, 2006

What is the Alert Indicator?

The Alert Indicator shows the current level of malicious cyber activity and reflects the potential for, or actual damage. The indicator consists of 5 levels:

1. Low **Green or Low** – Indicates a low risk. No unusual activity exists beyond the normal concern for known hacking activities, known viruses or other malicious activity.

   Examples:
   - Normal probing of the network
   - Low risk viruses

   Actions:
   - Continue routine preventative measures including application of vendor security patches and updates to anti-virus software signature files on a regular basis.
   - Continue routine security monitoring.
   - Ensure personnel receive proper training on Cyber Security policies.

   Notification:
   - No notification is warranted if a State is currently at this level.
   - Notification via the Multi-State ISAC's web site will be done concurrently with the Alert Level change.

2. Guarded **Blue or Guarded** – Indicates a general risk of increased hacking, virus or other malicious activity. The potential exists for malicious cyber activities, but no known exploits have been identified, or known exploits have been identified but no significant impact has occurred.

   Examples:
   - A critical vulnerability is discovered but no exploits are reported.
   - A critical vulnerability is being exploited but there has been no significant impact.
   - A new virus is discovered with the potential to spread quickly.
   - Credible warnings of increased probes or scans.
   - Compromise of non-critical system(s) that did not result in loss of data.

Actions:

- Continue recommended actions from previous level.
- Identify vulnerable systems.
- Implement appropriate counter-measures to protect vulnerable systems.
- When available, test and implement patches, install anti-virus updates, etc. in next regular cycle.

Notification:

- Notification via Multi-State ISAC's web site will be done concurrently with the Alert Level change.

3. **Elevated** **Yellow or Elevated** – Indicates a significant risk due to increased hacking, virus or other malicious activity which compromises systems or diminishes service. At this level, there are known vulnerabilities that are being exploited with a moderate level damage or disruption, or the potential for significant damage or disruption is high.

Examples:

- An exploit for a critical vulnerability exists that has the potential for significant damage.
- A critical vulnerability is being exploited and there has been moderate impact.
- Compromise of secure or critical system(s) containing sensitive information.
- Compromise of critical system(s) containing non-sensitive information if appropriate.
- A virus is spreading quickly throughout the Internet causing excessive network traffic.
- A distributed denial of service attack.

Actions:

- Continue recommended actions from previous levels.
- Identify vulnerable systems.
- Increase monitoring of critical systems.
- Immediately implement appropriate counter-measures to protect vulnerable critical systems.
- When available, test and implement patches, install anti-virus updates, etc. as soon as possible.

Notification:

- Notification to the Multi-State ISAC **via secure portal e-mail or telephone** will be given when a State upgrades its Alert Level to **Yellow or Elevated**.

- Notification via the Multi-State ISAC’s web site will be done concurrently with the Alert Level change.
- Notification via secure portal e-mail will be sent to the States when the any state or the national alert level is raised to **Yellow or Elevated.**

4. High **Orange or High** – Indicates a high risk of increased hacking, virus or other malicious cyber activity which targets or compromises core infrastructure, causes multiple service outages, multiple system compromises or compromises critical infrastructure. At this level, vulnerabilities are being exploited with a high level of damage or disruption, or the potential for severe damage or disruption is high.

Examples:

- An exploit for a critical vulnerability exists that has the potential for severe damage.
- A critical vulnerability is being exploited and there has been significant impact.
- Attackers have gained administrative privileges on compromised systems.
- Multiple damaging or disruptive virus attacks.
- Multiple denial of service attacks against critical infrastructure services.

Actions:

- Continue recommended actions from previous levels.
- Closely monitor security mechanisms including firewalls, web log files, anti-virus gateways, system log files, etc. for unusual activity.
- Consider limiting or shutting down less critical connections to external networks such as the Internet.
- Consider isolating less mission critical internal networks to contain or limit the potential of an incident.
- Consider use of alternative methods of communication such as phone, fax or radio in lieu of e-mail and other forms of electronic communication.
- When available, test and implement patches, anti-virus updates, etc. immediately.

Notification:

- Notification to the Multi-State ISAC via secure portal **e-mail or telephone** will be given when a State upgrades its Alert Level to **Orange or High.**
- Notification via the Multi-State ISAC’s web site will be done concurrently with the Alert Level change
- Notification via secure portal e-mail will be sent to the States when any state or the national alert level is raised to **Orange or High.**

5. Severe **Red or Severe** – Indicates a severe risk of hacking, virus or other malicious activity resulting in wide-spread outages and/or significantly destructive compromises to systems with no known remedy or debilitates one or more critical infrastructure sectors. At this level, vulnerabilities are being exploited with a severe level or wide spread level of damage or disruption of Critical Infrastructure Assets.

Examples:

- Complete network failures.
- Mission critical application failures.
- Compromise or loss of administrative controls of critical system.
- Loss of critical supervisory control and data acquisition (SCADA) systems.
- Potential for or actual loss of lives or significant impact on the health or economic security of the State.

Actions:

- Continue recommended actions from previous levels.
- Shutdown connections to the Internet and external business partners until appropriate corrective actions are taken.
- Isolate internal networks to contain or limit the damage or disruption.
- Use alternative methods of communication such as phone, fax or radio as necessary in lieu of e-mail and other forms of electronic communication.

Notification:

- Notification **via secure portal e-mail, telephone, pager, or fax** will be given when a State upgrades its Alert Level to **Red or Severe.**
- Notification via the Multi-State ISAC's web site will be done concurrently with the Alert Level change.
- Notification to the States via secure portal e-mail or telephone to set up conference call when the Multi-State ISAC upgrades the national alert level to **Red or Severe.**

What are Critical Infrastructure Assets?

** For the purposes of this process, critical infrastructure assets are being defined as follows:*

Critical Infrastructure Assets are physical and/or logical assets which are so vital that their infiltration, incapacitation, destruction or misuse would have a debilitating impact on the health, safety, welfare or economic security of the citizens and businesses of the State.

Process for Determining Alert Indicator Level

The appropriate Alert Indicator Level is determined using the following threat severity formula[1]:

Severity = (Criticality + Lethality) – (System Countermeasures + Network Countermeasures)

Where the value of criticality, lethality, system countermeasures and network countermeasures are as follows:

Criticality: What is the target of the attack?

Value	Target
5	Core services such as critical routers, firewalls, VPNs, IDS systems, DNS servers or authentication servers (e.g. LDAP)
4	E-mail, web, database and critical application servers.
3	Less critical application servers.
2	Business desktop systems.
1	Home users.

Lethality: How likely will the attack do damage?

Value	Potential Damage
5	▪ Exploit exists. ▪ Attacker could gain root or administrator privileges. ▪ Attacker could commit denial of service.
4	▪ Exploit exists. ▪ Attacker could gain user level access privileges. ▪ Attacker could commit denial of service.
3	▪ No known exploit exists. ▪ Attacker could gain root or administrator privileges. ▪ Attacker could commit degradation of service.
2	▪ No known exploit exists. ▪ Attacker could gain user level access privileges.
1	▪ No known exploit exists. ▪ Attacker could not gain access.

System Counter-Measures: What host-based preventative measures are in place?

Value	Countermeasure
5	▪ Current operating system with applicable patches applied.

[1] **1. Based on the formula by Stephen Northcutt from the SANS Institute**

	▪ Server has been hardened and verified via vulnerability scan. ▪ Running host-based IDS or integrity checker. ▪ Anti-virus signature exists and has been applied to target systems.
4	▪ Current operating system with applicable patches applied. ▪ Operating system has been hardened. ▪ Anti-virus signature exists and has been applied to target systems.
3	▪ Current operating system with fairly up-to-date patches applied. ▪ Anti-virus signatures are current.
2	▪ Current operating system but missing some applicable patches. ▪ Anti-virus signature either does not exist or has not been applied to target systems.
1	▪ Older operating systems including Windows NT 3.51, Solaris 2.6, Windows 95/98/ME. ▪ No anti-virus software protection.

Network Counter-Measures: What network-based preventative measures are in place?

Value	Countermeasure
5	▪ Restrictive (i.e. deny all except what is allowed) firewall. ▪ Firewall rules have been validated by penetration testing. ▪ All external connections including VPNs go through (not around) the firewall ▪ Network-based IDS is implemented. ▪ E-mail gateway filters attachments used by this virus.
4	▪ Restrictive firewall. ▪ External connections (VPNs, Wireless, Internet, Business partners, etc) are protected by a firewall. ▪ E-mail gateway filters attachments used by this virus.
3	▪ Restrictive firewall. ▪ E-mail gateway filters common executable attachments.
2	▪ Permissive firewall (i.e. “accept all but …”) or allowed service (e.g. HTTP, SMTP, etc) ▪ E-mail gateway does not filter all attachments used by this virus.
1	▪ No firewall implemented. ▪ E-mail gateway does not filter any attachments.

Using the result from the formula defined above, the Alert Indicator would generally reflect severity levels as follows:

Alert Indicator Level	**Severity**
Green – Low	-8 to -5
Blue – Guarded	-4 to -2
Yellow – Elevated	-1 to +2
Orange – High	+3 to +5
Red – Severe	+6 to +8

Note that these are guidelines. Other conditions, on a case by case basis, may be factored into determining the final Alert Indicator Level.