

Information Technology Resource Management Council (ITRMC)

ENTERPRISE GUIDELINES – G500 SECURITY PROCEDURES

Category: G520 – CYBER SECURITY ALERT INDICATOR

CONTENTS:

- I. [Definition](#)
- II. [Rationale](#)
- III. [Reference](#)
- IV. [Guideline](#)
- V. [Timeline](#)

I. DEFINITION

1. Cyber Alert Indicator – Indicator scale set to demonstrate the current level of malicious cyber activity and reflect the potential for (or actual) damage.
2. Critical Infrastructure Assets – 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.
3. Cyber Security Incident – Any adverse event that threatens the confidentiality, integrity or accessibility of an agency's information resources. These events include, but are not limited to, the following:
 - A. Attempts (either failed or successful) to gain unauthorized access to a system or its data;
 - B. Disruption or denial of service;
 - C. Unauthorized use of a system for the transmission, processing or storage of data;
 - D. Changes to system hardware, firmware or software without the agency's knowledge, instruction or consent;
 - E. Attempts to cause failures in critical infrastructure services or loss of critical supervisory and data acquisition (SCADA) systems;
 - F. Attempts to cause failures that may cause loss of life or significant impact on the health or economic security of the agency and/or State; and
 - G. Probing of any nature that an agency or other authorized entity has not approved in advance for system security testing purposes.

II. RATIONALE

This guideline outlines the definitions for the various Cyber Alert Indicator levels and specifies the procedures for setting a specific level. It also provides guidance on how the Cyber Alert Indicator will be communicated to agencies and the Multi-State Information Sharing and Analysis Center (MS-ISAC) as part of the National Cyber Alert Indicator program.

III. REFERENCE

ITRMC [Policy 4110 – IT Security Coordinator](#); and

ITRMC [Policy 4510 – Cyber Security Incident Reporting](#).

IV. GUIDELINE

1. The Cyber Alert Indicator will be set according to the criteria set forth within this guideline. Any changes to the indicator will be promptly communicated to Agency IT Security Coordinators.
 - A. Upon notification of changes to the Cyber Alert Indicator, Agency IT Security Coordinators should review the recommended agency actions for the specified alert level and take action, as deemed necessary; and
 - B. The indicator will be reviewed and updated weekly or as circumstances warrant (e.g., cyber security incident).
2. The Cyber Alert Indicator is comprised of five levels (based upon the recommendations from the National Cyber Alert Indicator program). The following criteria set forth the recommended agency actions and notification procedures for each alert level:
 - A. Low (Green) – Indicates a low risk. No unusual activity exists beyond the normal concern for known hacking activities, known viruses or other malicious activity.
 - (1) Examples:
 - (a) Normal probing of the State's network; or
 - (b) Low risk viruses.
 - (2) Recommended Agency Actions:
 - (a) Continue routine preventative measures, including application of vendor security patches and updates to anti-virus software signature files on a

regular basis;

(b) Continue routine security monitoring; and

(c) Ensure personnel receive proper training on Cyber Security policies.

(3) Notification:

(a) No notification is warranted to Agency IT Security Coordinators or to the MS-ISAC when the State remains at this level;

(b) Notification via e-mail to Agency IT Security Coordinators and to the MS-ISAC will be given when the State downgrades from a higher alert level to this level; and

(c) The Statewide Cyber Security Coordinator (or alternate) will update the State's status within the National Cyber Alert Indicator System when transitioning to this level.

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

(1) Examples:

(a) A critical vulnerability is discovered and exploit code has been identified;

(b) A critical vulnerability is being exploited but there has been no significant impact;

(c) A new virus is discovered with the potential to spread quickly; or

(d) Credible warnings of increased probes or scans to the State's network.

(2) Recommended Agency Actions:

(a) Continue recommended actions from previous level;

(b) Identify vulnerable systems; and

(c) Implement appropriate counter-measures to protect vulnerable systems.

(3) Notification:

(a) Notification via e-mail to the Agency IT Security Coordinators and to the

MS-ISAC will be given when the State upgrades or downgrades to this level; and

- (b) The Statewide Cyber Security Coordinator (or alternate) will update the State's status within the National Cyber Alert Indicator System when transitioning to this level.

C. Elevated (Yellow) – Indicates a significant risk due to increased hacking, virus or other malicious activity which compromises systems or diminishes service. Known vulnerabilities are being exploited with a moderate level of damage or disruption, or the potential for significant damage or disruption is high.

(1) Examples:

- (a) An exploit for a critical vulnerability exists that has the potential for significant damage;
- (b) A critical vulnerability is being exploited and there has been moderate impact;
- (c) Targeted web site defacement attempts or successes are occurring;
- (d) A virus is spreading quickly throughout the Internet causing excessive network traffic; or
- (e) A distributed denial of service attack is eminent or occurring.

(2) Recommended Agency Actions:

- (a) Continue recommended actions from previous level;
- (b) Identify vulnerable systems;
- (c) Increase monitoring of critical systems;
- (d) Immediately implement appropriate counter-measures to protect vulnerable systems; and
- (e) When available, test and implement patches and/or install antivirus updates, as soon as possible.

(3) Notification:

- (a) Notification via e-mail and telephone (voice mail message is acceptable) to the Agency IT Security Coordinators and to the MS-ISAC will be given when the State upgrades to this level;

- (b) Notification via e-mail only will be given to the Agency IT Security Coordinators and to the MS-ISAC when the State downgrades to this level; and
 - (c) The Statewide Cyber Security Coordinator (or alternate) will update the State's status within the National Cyber Alert Indicator System when transitioning to this level.
- D. High (Orange) – 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.
- (1) Examples:
- (a) An exploit for a critical vulnerability exists that has the potential for severe damage;
 - (b) A critical vulnerability is being exploited and there has been significant impact;
 - (c) Attackers have gained administrative privileges on compromised systems;
 - (d) Multiple damaging or disruptive virus attacks are occurring; or
 - (e) Multiple denial of service attacks against critical infrastructure services are occurring.
- (2) Recommended Agency Actions:
- (a) Continue recommended actions from previous level;
 - (b) Closely monitor security mechanisms including firewalls, web log files, anti-virus gateways, system log files, and other devices for unusual activity;
 - (c) Consider limiting or shutting down less critical connections to external networks, such as the Internet or to other state entities;
 - (d) Consider isolating less mission critical internal networks to contain or limit the potential of an incident;
 - (e) Consider use of alternative methods of communication such as phone, fax or radio in lieu of e-mail and other forms of electronic communication; and

- (f) When available, test and implement patches and/or install antivirus updates, as soon as possible.

(3) Notification:

- (a) Notification via telephone (voice mail message is acceptable) to the Agency IT Security Coordinators and to the MS-ISAC will be given when the State upgrades to this level;
- (b) Notification via e-mail only will be given to the Agency IT Security Coordinators and to the MS-ISAC when the State downgrades to this level; and
- (c) The Statewide Cyber Security Coordinator (or alternate) will update the State's status within the National Cyber Alert Indicator System when transitioning to this level.

E. Severe (Red) – 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.

(1) Examples:

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

(2) Recommended Agency Actions:

- (a) Continue recommended actions from previous level;
- (b) Closely monitor security mechanisms including firewalls, web log files, anti-virus gateways, system log files, and other devices for unusual activity;
- (c) Shutdown connections to the Internet, external business partners, and other state entities until appropriate corrective actions are taken;

- (d) Isolate internal networks to contain or limit the damage or disruption; and
 - (e) Use alternative methods of communication such as phone, fax or radio in lieu of e-mail and other forms of electronic communication.
- (3) Notification:
- (a) Notification via telephone to the Agency IT Security Coordinators and to the MS-ISAC will be given when the State upgrades to this level. If cell phone and/or pager information is on file for the Agency IT Security Coordinator, the notification will also be transmitted through that channel;
 - (b) The Statewide Cyber Security Coordinator (or alternate) will update the State's status within the National Cyber Alert Indicator System when transitioning to this level; and
 - (c) Notification when downgraded.

V. TIMELINE

Last Revised:

Effective Date: April 25, 2005