State of New Mexico Statewide Architectural Configuration Requirements
Title: Incident Response and Reporting Standard
S-STD-012.001
Effective Date: August 19, 2005

1. Authority

The Department of Information Technology (DoIT) shall develop, implement and maintain a coordinated statewide plan for information technology (IT) including the adoption of statewide technical, coordination, and security standards per the Department of Information Technology Act, NMSA 9-27-1 et. seq. (1978).

2. Purpose

This standard defines Agency responsibilities for responding to and reporting cyber-attacks and for sharing information related to potential incidents or threats with the State's Computer Security Incident Response Team (CSIRT) and the Chief Information Security Officer (CISO).

3. Scope

This applies to all agencies. An agency is defined as a department, commission, board, institution or other agency of the state organization receiving, expending or disbursing state funds or incurring obligations of the state including the board of regents and the state board of directors for community colleges but excluding the universities under the jurisdiction of the board of regents and the community colleges under their respective jurisdictions and the legislative or judicial branches.

The Agency Chief Executive Officer (CEO), working in conjunction with the Agency Chief Information Officer (CIO), shall be responsible for ensuring the effective implementation of Statewide Information Technology Policies, Standards, and Procedures within each agency.

4. Standard

To secure and protect the State of New Mexico's critical IT business processes and assets from cyber-security incidents (i.e. cyber-crime or cyber-terrorism), agencies shall report all incidents to the Statewide CSIRT within 24 hours of the incident or next business day.

4.1. CYBER SECURITY INCIDENTS**:** Agencies shall report any of the following acts by any person who, without authority or acting in excess of authority:

- Unauthorized access or theft of an IT device (server, storage, or client) or network with the intent to instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system, or network;
- Accesses, alters, damages, steals, misappropriates, or destroys any IT device, network, or any physically or logically connected IT devices;
- Accesses, alters, damages, or destroys any computer application systems programs, or data, especially for personal use;
- Recklessly disrupts or causes the disruption of any services provided through the use of any IT device or network;
- Denies or causes the denial of IT-related services to any authorized user of those services;
- Recklessly uses an IT device or network to engage in a scheme or course of conduct that is directed toward another person and that seriously alarms, torments, threatens, or terrorizes the person;
- Prevents a computer user from exiting an Internet, Intranet, or internal host site, computer system, or network-connected location in order to compel the user's computer to continue communicating with, connecting to, or displaying the content of the service, site, or system;
- Knowingly obtains any information that is required by law to be kept confidential or any records that are not classified as public records by accessing an IT device or network that is operated by the State, a political subdivision of the State, or a medical institution;
- Introduces a computer-related contaminant (e.g., malicious code, virus, worm, etc.) into any IT device or network; and
- Makes multiple attempts to access an IT device or network system within a brief period of time.

4.2 CYBER INCIDENT REPORTING – The Agency shall notify CSIRT within 24 hours of the incident or next business day of detecting the incident by whatever means of communication is both available and fastest (i.e., phone, fax, e-mail, courier).

- The following information, at a minimum, is required when reporting intrusions to CSIRT:
    - Agency name;
    - The Agency CSIRT Coordinator's name and phone number (see 4.6); and
    - Brief description of intrusion and damages (real or anticipated).

- Whenever possible, the Agency should capture and maintain log entries for a minimum of one week following the detection of intrusion (or longer at the discretion of the application or system owner). Log entries provide significant detail that can be used for investigation and prosecution of the intruder.

4.3. CSIRT INCIDENT REPORT – After notifying CSIRT of the intrusion, the Agency shall complete a CSIRT Incident Report available on the DoIT's web page http://www.doit.state.nm.us/securityoffice.html/forms/it_asset_incident_report.doc. The Agency representative completing the report should provide as much detail as possible in the remarks fields and annotate the description of the intrusion with explanatory remarks. As more information becomes available or the situation changes, the Agency shall revise and re-submit the incident report to CSIRT with a clear date-time stamp.

4.4. CSIRT ESCALATON PROCESS – In the event of personal harm or potential financial damage from an intrusion, CSIRT will be in constant contact with the CSIRT Coordinator or designee at the affected Agency, the Department of Public Safety, the Attorney General's Office, and other organizations, as necessary, until resolution and recovery efforts have been completed. The agency CEO will be responsible for final decisions affecting the final incident resolution.

4.5. CSIRT ALERT NOTIFICATIONS

4.5.1. **CSIRT Responsibilities –** As CSIRT enterprise member DoIT creates or receives computer security alerts, it shall forward them to agency CIOs or designees. Each alert shall state, as a minimum, the identity of the risk, level of risk, and any available patches or inoculants to mitigate the risk.

4.5.2. **Agency Responsibilities --** Upon receiving a CSIRT alert, the agency CIOs or designees shall notify agency personnel about the alert. The CIO shall send alert notifications by email and determine whether to send it to all employees, specific divisions within the agency, or specific individuals; depending on the content.

4.6. CSIRT MEMBERSHIP – Each agency shall assign an individual as a member of CSIRT. The agency CIO or designee shall complete a CSIRT membership application and deliver it to CSIRT. The agency CIO or designee shall ensure that the contact information remains current and apprise CSIRT of any changes.

5. Definitions

Refer to the N-DEF001.001 Glossary of Terms located on the DoIT website: http://www.doit.state.nm.us/standards.html

6. References

Internet, Intranet, Email, and Digital Network Usage, NMAC 1.12.10
Enterprise Architecture, NMAC 1.12.11
Information Security Operation Management, NMAC 1.12.20

7. Attachments

None

8. Version Control

S-STD-012.001

9. Revision History

Original 08/19/05
Format Updated 09/19/13