MEETING AGENDA

State Government Council
of the
Nebraska Information Technology Commission

Thursday, February 14, 2008
1:30 p.m. - 2:30 p.m.
Executive Building - Lower Level Conference Room
521 S 14th Street
Lincoln, Nebraska

AGENDA

Meeting Documents: Click the links in the agenda
or click here for all documents. (xx Pages)

1. Roll Call, Meeting Notice & Open Meetings Act Information

2. Public Comment

3. Approval of Minutes* - January 10, 2008

4. Standards and Guidelines

   - Update on documents discussed at the January meeting
     - NITC 1-204: IT Procurement Review Policy - Attachment A (Revised)
   - Recommendations to the NITC*
     - NITC 8-401: Incident Response and Reporting Standard (Revised)

5. Updated Statewide Technology Plan Action Items*

6. Demonstration - Department of Environmental Quality - Dennis Burling

7. Other Business

8. Agency Reports

9. Next Meeting Date - March 13, 2008

10. Adjourn

* Denotes action items.

(The Council will attempt to adhere to the sequence of the published agenda, but reserves the right to adjust the order of items if necessary and may elect to take action on any of the items listed.)

NITC and State Government Council Websites: http://nitc.ne.gov
Meeting notice was posted to the NITC Website and Nebraska Public Meeting Calendar on January 11, 2008.
The agenda posted to the NITC Website on February 10, 2008.

MEETING MINUTES

STATE GOVERNMENT COUNCIL
Nebraska Information Technology Commission
Thursday, January 10, 2008, 1:30 p.m.
Executive Building-Lower Level Conference Room
521 South 14th Street, Lincoln, Nebraska
PROPSED MINUTES

MEMBERS PRESENT:

Tom Conroy, OCIO-Enterprise Computing Services
Josh Daws, Secretary of State's Office
Brenda Decker, Chief Information Officer
Keith Dey, Department of Motor Vehicles
Pat Flanagan, Private Sector
Rex Gittins, Department of Natural Resources
Dorest Harvey, Private Sector
Jeanette Lee, Department of Banking
Bill Miller, State Court Administrator's Office
Glenn Morton, Workers' Compensation Court
Mike Overton, Crime Commission
Jayne Scofield, OCIO - Network Services
Bob Shanahan, Department of Labor
Len Sloup, Department of Revenue
Bill Wehling, Department of Roads
George Wells, Department of Correctional Services

MEMBERS ABSENT: Bob Beecham, NDE Support Services; Dennis Burling, Department of Environmental Quality; Mike Calvert, Legislative Fiscal Office; Carlos Castillo, Department of Administrative Services; Lauren Hill, Governor's Policy Research Office; Jim Ohmberger, Health and Human Services; Gerry Oligmueller, Budget Office; Terry Pell, State Patrol; and Rod Wagner, Library Commission

ROLL CALL, MEETING NOTICE & OPEN MEETINGS ACT INFORMATION

Ms. Decker called the meeting to order at 1:30 p.m. There were 14 voting members at the time of roll call. It was stated that the meeting notice was posted to the NITC, State Government Council and Nebraska Public Meeting Calendar Websites on November 29, 2007 and that the agenda posted to the NITC Website on December 21, 2007. A copy of the Open Meetings Act was located on the front table.

PUBLIC COMMENT

There was no public comment.

Rex Gittins arrived at the meeting.

APPROVAL OF NOVEMBER 20, 2007 MINUTES

Mr. Harvey moved to approve the November 20, 2007 minutes as presented. Mr. Shanahan seconded. Roll call vote: Conroy-Yes, Decker-Yes, Sloup-Yes,

Flanagan-Yes, Daws-Yes, Gittins-Yes, Harvey-Yes, Shanahan-Yes, Lee-Yes, Morton-Abstain, Dey-Yes, Scofield-Yes, George Wells-Yes, Miller-Yes, and Wehling-Yes. Results: Yes-14, No-0, Abstain-1. Motion carried.

Due to a scheduling conflict, the Department of Environmental Quality will not be providing the demonstration listed in the agenda.

STANDARDS AND GUIDELINES - RECOMMENDATIONS TO THE TECHNICAL PANEL AND NITC*

NITC 01-101: Definitions

There were no recommended changes from the member. Mr. Morton stated that he will be abstaining during the roll call vote due to applicability on the first three standards and guidelines.

Mr. Shanahan moved to recommend approval of NITC 01-101: Definitions. Mr. Flanagan seconded. Roll call vote: Wehling-Yes, Miller-Yes, Wells-Yes, Scofield-Yes, Dey-Yes, Morton-Abstain, Lee-Yes, Shanahan-Yes, Harvey-Yes, Gittins-Yes, Daws-Abstain, Flanagan-Yes, Sloup-Yes, Decker-Yes, and Conroy-Yes. Results: Yes-13, No-0, Abstain-2. Motion carried.

NITC 01-103: Waiver Policy

It was suggested to have a generic email address for agencies to submit requests.

Mr. Conroy moved to recommend approval of NITC 01-103: Waiver Policy. Mr. Wells seconded. Roll call vote: Shanahan-Yes, Lee-Yes, Harvey-Yes, Morton-Abstain, Gittins-Yes, Dey-Yes, Daws-Yes, Scofield-Yes, Flanagan-Yes, Wells-Yes, Sloup-Yes, Miller-Yes, Conroy-Yes, Wehling-Yes, and Decker-Yes. Results: Yes-14, No-0, Abstain-1. Motion carried.

NITC 01-204: IT Procurement Review Policy

Per statutes, the Office of the CIO is required to approve IT related purchases. This policy is intended to document the review process and provide a list of preapproved items.

A question was raised about including replacement parts for existing equipment in the preapproved list. Ms. Decker stated that other agencies have asked for this also and it is being considered for inclusion by the OCIO.

It was suggested that there should be a dollar limit on the preapproved items.

Mike Overton arrived at the meeting.

Ms. Lee moved that the council table any action until the next meeting. Mr. Wells seconded.

Discussion followed regarding approval of the policy versus the preapproved list in Attachment A. Ms. Decker stated that the current discussion is only to consider recommending approval of the policy. The list in Attachment A can be revised by the CIO.

The question was raised regarding incorporating the list in NIS so that agencies are allowed to purchase without CIO review and approval. Amy Archuleta was present and state that NIS can be revised to meet these needs.

Ms. Lee and Mr. Wells withdrew their motion.

Mr. Shanahan moved to recommend approval of NITC 01-204: IT Procurement Review Policy. Mr. Dey seconded. Roll call vote: Shanahan-Yes, Lee-Yes, Morton-Abstain, Dey-Yes, Scofield-Yes, George Wells-Yes, Miller-Abstain, Wehling-Yes, Overton-Yes, Conroy-Yes, Decker-Yes, Sloup-Yes, Flanagan-Yes, Daws-Abstain, Gittins-Yes, and Harvey-Yes. Results: Yes-13, No-0, Abstain-3. Motion carried.

NITC 08-401: Incident Response and Reporting Standard | Reporting Form

Mr. Hartman reviewed changes, including a new reporting form.

Members had questions about the types of incidents for which reporting is required and the training requirements.

Mr. Wehling moved to table consideration of NITC 08-401: Incident Response and Reporting Standard until the February meeting. Mr. Wells seconded. Roll call vote: Harvey-Yes, Gittins-Yes, Daws-Yes, Flanagan-Yes, Sloup-Yes, Decker-Yes, Conroy-Yes, Overton-Yes, Wehling-Yes, Miller-Yes, Wells-Yes, Scofield-Yes, Dey-Yes, Morton-Yes, Lee-Yes, Shanahan-Yes. Results: Yes-16, No-0. Motion carried.

UPDATE ON EMAIL CONVERSION

IronPort: An Office of the CIO staff member is receiving training on IronPort. Council members were asked to continue using the CIO Help Desk to report issues.

Efax: Dynamic Solutions has been contacted about supporting this application. An agreement is being drafted.

Conversion Update: Approximately, 1,800 accounts have been converted. Stan Schmidt will follow-up on requested testing by the Workers Compensation Court. The Project is working with the Secretary of State’s Office regarding records retention.

NEXT MEETING DATE, TIME AND LOCATION AND MEETING ADJOURNMENT

The next meeting of the NITC State Government Council will be held at 1:30 p.m. on February 14. The location will be determined at a later time.

Mr. Flanagan moved to adjourn. Mr. Daws seconded. All were in favor. Motion carried by unanimous voice vote.

The meeting was adjourned at 3:11 p.m.

Meeting minutes were taken by Lori Lopez Urdiales and reviewed by Rick Becker of the Office of the CIO.

NITC 1-204
Attachment A

Office of the CIO

List of Preapproved Items for Purchase

For the purpose of procurement reviews conducted pursuant to NEB. REV. STAT. §§ 81-1117, 81-1120.17 and 81-1120.20, the following items are preapproved for purchase by agencies, if the cost of the item is less than $500.00:

1. Functionally equivalent parts needed to repair existing equipment
2. Cables for connecting computer components
3. Power Cords / Adapters
4. Extender Cables for Keyboards / Mice
5. KVM (Keyboard - Video - Mouse) Switches
6. USB / PS2 Connectors
7. Memory Chips
8. Laptop Batteries
9. Laptop Docking Stations
10. UPS (Uninterruptible Power Supply)
11. Keyboards
12. Mice
13. Speakers
14. Monitors that are ordered without a system
15. Hard Drives
16. CD/DVD Drives
17. Video Cards
18. Network Cards
19. Barcode Pens and Readers
20. Card Readers
21. Smart Board Overlays
22. Projectors and Projector Lamps
23. Desktop Printers
24. Printer Toner and Ink
25. Desktop Scanners
26. Small Label Printers
27. Blank CDs or DVDs
28. Blank Tapes
29. Digital Voice Recorders
30. Flash Drives
31. Software Books
32. Training CDs or DVDs
33. Logic boards and computers that are integral parts of equipment that serves a primary purpose other than information management, including digital cameras, lab equipment, and motor vehicles.

Formatted: Bullets and Numbering

Date of Last Revision: February 11, 2008
[The current version of this document is available at: http://nitc.ne.gov/standards/xxx.htm]

Deleted: November 28, 2007

Nebraska Information Technology Commission

STANDARDS AND GUIDELINES

Incident Response Standard

Category	**Security Architecture**
Title	**Incident Response Standard**
Number	

Applicability	☑ State Government Agencies ☐ **All** .... Not Applicable ☑ **Excluding <u>higher education institutions</u>** ....Standard ☐ State Funded Entities - **All entities receiving state funding for matters covered by this document** .... Not Applicable ☑ Other: **All Public Entities**............................Guideline **Definitions:** **Standard** - Adherence is required. Certain exceptions and conditions may appear in this document, all other deviations from the standard require prior approval of ___________. **Guideline** - Adherence is voluntary.

Status	☐ **Adopted** ☐ **Draft** ☐ **Other:________**
Dates	**Date:** **Date Adopted by NITC:** **Other:**

Prepared by: Technical Panel of the Nebraska Information Technology Commission
Authority: Neb. Rev. Stat. § 86-516(6)
http://www.nitc.state.ne.us/standards/

1. Purpose and Objectives

Computer systems are subject to a wide range of mishaps; from corrupted data files, to viruses, to natural disasters. These mishaps can occur at anytime of the day or night. Many mishaps are fixed through day-to-day operating procedures, while more severe mishaps are addressed in other plans, e.g. Continuity of Operations (COOP) plans. In some cases, incident handling actions will not be performed by a single person or on a single system. Responses to an incident can range from recovering compromised systems to the collection of evidence for the purpose of criminal prosecution. Therefore, preparation and planning for incidents, and ensuring the right resources are available, are critical to an agencies ability to adequately detect, respond and recover.

A formally documented and coordinated incident response capability is necessary in order to rapidly detect incidents, minimize loss and destruction, mitigate exploited weaknesses, and restore computing services. It prepares agencies to: efficiently respond, protect systems and data, and prevent disruption of services across multiple platforms and between agencies across the State network. Incorporated within these standards are accepted best practices within the law enforcement and Information Technology (IT) security communities. These standards will facilitate cooperation and information exchange among those responsible for responding to and reporting on incidents on any State of Nebraska information system.

2. Standard

It is the responsibility of all State of Nebraska agencies that support information systems to develop, disseminate, and periodically review/update a formal, documented, incident response capability that includes preparation, analysis, containment, eradication, and recovery. In addition, lessons learned from prior and ongoing incident activities should be incorporated into the incident response capability. Agency plans should cover all potential types of incidents, including but not limited to:

- Information system failures and loss of service;
- Denial of service;
- Breaches of confidentiality

In addition to plans that recover systems or services as quickly as possible, the plan should also cover:

- Analysis and identification of the cause;
- Planning and implementation of remedies to prevent recurrence, if necessary;
- Collection of audit trails and similar evidence;
- Communication with those either affected by or potentially affected by the incident; and
- Reporting the incident

2.1 Incident Response Team

Agencies should identify knowledgeable staff that can rapidly respond to, manage, and support any suspected incident to minimize damage to State information system(s), network(s) and data by identifying and controlling the incident, properly preserving evidence, and reporting to appropriate entities. An agency contact list should be developed and maintained for incident response personnel, which includes the names, telephone numbers, pager numbers, mobile telephone numbers, e-mail addresses, organization names, titles, and roles and responsibilities for all key incident response resources, including but not limited to agency personnel and management, other key state agencies, vendors, and contacts.

2.2 Initiate an Incident Log

Documentation of information is critical in situations that may eventually involve authorities, as well as provides a historical event of the actions taken to resolve the event. Manually written incident logs are preferable since electronic logs can be altered or deleted. The minimum information that should be recorded is:

- When (date and time) and how the incident was reported, discovered or occurred;
- Who reported or discovered the incident;
- Description of the incident;
- Incident-related tasks and who performed each, and the amount of time spent on each task;
- Individuals contacted regarding the incident; and
- Information system(s), program(s) or network(s) affected.

2.3 Classification of Incidents

The agency Information Security Officer (ISO) should review the incident information to determine if an actual incident has occurred. Incidents are classified into four tiers based on the severity of the incident: Tier 1, Tier 2, Tier 3, or Tier 4.

Tier	Definition	Examples	Report to SISO	Activate Agency IRP
1	Localized, minor incidents. Non-critical systems.	- Localized virus attacks - Internet abuse that results in disciplinary action, excluding criminal behavior - Incidents traceable to user error or system failure - Sustained attempts at intrusion, scanning or pinging of state devices - Missing IT devices or equipment with storage capabilities	Report to the SISO within one business day	No
2	Incidents affecting critical systems or information; or affecting more than one agency.	- Coordinated, distributed attacks - Any attack which causes Denial of Service - Financial fraud - Unauthorized activity involving a server, host, or Confidential system (HR, Legal, Financial, etc.) - Theft of proprietary information - Internet abuses violating Federal/ State law - Theft of IT devices with storage capabilities	Report verbally to the SISO immediately for determination of escalation, and/or assistance.	Yes
3	Incidents impacting multiple agencies	- Service provider outage - Core network outage - Mainframe outage	Report verbally to the SISO immediately.	Yes
4	Governor declared emergency	- Activation of COOP Plan	No	As directed

Deleted: verbally

Deleted: Minor

2.4 Cyber Security Incidents

Each agency shall securely maintain any information collected, generated, or assessed in the course of determining whether an incident is a potential cyber security incident warranting prosecution. Data collection shall focus on identifying who, what, when, where, and the how of an incident. Collected information shall be properly documented and safeguarded. Evidence such as system and network log files, user files, system administrator logs and notes, backup-up tapes, and intrusion detection system logs, alarms or alerts shall be securely maintained and the chain of custody preserved by:

- Ensuring the evidence has not been altered;
- Ensuring the evidence is accounted for at all times;
- Verifying the passage of evidence from one party to another is fully documented; and
- Verifying the passage of evidence from one location to another is fully documented.

If an incident is determined not to be a cyber security incident, agencies are still required to maintain any evidence and its chain of custody because future incidents may require the previously captured evidence.

2.4.1 Security Incident Evidence File

An evidence file shall be created to record and maintain an inventory of all actions taken, action timestamps and correspondence associated with a security incident.

2.4.2 Notification of Personal Information Security Breach

Agencies shall determine if the incident resulted in a breach to a system containing personal information and then notify affected individual as required by Neb. Rev. Stat. § 84.121 or other State or Federal regulatory guidelines.

2.4.3 Security Incident Confidentiality

Communication shall be on a need-to-know basis and shall be considered confidential during a security incident investigation. Incident responders are not to share any details with anyone other than the Incident Response team, agency management or the State Information Security Officer (SISO) (see Section 2.12)

2.5 Reporting to the State Information Security Officer

Agencies shall report incident information to the SISO. The SISO will contact appropriate authorities in accordance with State or Federal incident reporting procedures, applicable laws, directives, policies, regulations, standards, and procedures; and to US-Cert and law enforcement, if necessary. Reporting to the SISO does not relieve agencies from other reporting requirements.

The SISO has the responsibility to inform other agencies about incidents impacting multiple agencies that may become a potential threat.

2.6 Escalation Process

Agencies should periodically review the incident conditions and determine if escalation to a higher tier is appropriate. An incident may be escalated in any of the following ways:

- Determination by the Chief Information Officer or State Information Security Officer;
- Additional related events (i.e. emergence of a distributed, coordinated attack, etc.)
- Requested by agency management.

2.6.1 Escalation Thresholds

Agencies should consider escalating an incident when certain conditions are met. The following thresholds of incident actions are examples of when to consider incident escalation:

Deleted: actions,

- Multiple machines per LAN segment showing Intrusion Prevention System signature;
- Multiple machines showing multiple Intrusion Prevention System signatures;
- One or more critical infrastructure/application showing Intrusion Prevention system signatures;
- Significant impact on bandwidth;
- When a concerted effort is shown to be attacking the network, either internally or externally;
- Any known or reported compromise of Personal Identifiable Information (PII);
- Any website defacement.
- Abnormal increases in any of the above.

2.7 Response to Incidents

Priority in incident response is given to preventing further damage to State information systems. Therefore, the Office of the CIO reserves the right to quarantine any potentially threatening agency or system.

2.7.1 Incident Containment

Agencies shall identify containment strategies to control an incident’s impact to compromised systems, limit the extent of the incident, prevent further damage and regain normal operations of affected systems. Agency containment measures should take into consideration available resources, the classification of an incident, agency Continuity of Operations Plans (COOP) and procedures regarding response methods. Containment measures shall also be evaluated against the potential loss or corruption of security incident evidence. Containment methods shall include as a minimum:

- Ensuring redundant systems and data have not been compromised;
- Monitoring system and network activity;
- Disabling access to compromised shared file systems;
- Disabling specific system services;
- Changing passwords or disabling accounts;
- Temporarily shutting down the compromised or at risk system; and
- Disconnecting compromised or at risk systems from the network.

2.7.2 Incident Eradication

Agencies shall develop and employ mitigation strategies prior to returning compromised systems to service to protect against like or similar types of incidents in the future. Mitigation strategies may include, but are not limited to:

- Changing passwords on compromised systems;
- Disabling compromised accounts;
- Identifying and removing an intruder’s access method
- Installing system patches for known weaknesses or vulnerabilities;
- Adjusting or deploying firewall or intrusion detection system technologies to detect access and intrusion methods;
- Code changes to internal applications.

2.8 Recovery

Agencies shall evaluate and determine when to return compromised systems to normal operations. Access to compromised systems shall be limited to authorized personnel until the security incident has been contained and root cause mitigated. Analysis and mitigation procedures shall be completed as soon as possible, recognizing agency systems are vulnerable to other occurrences of the same type. Recovery procedures shall address:

- Recovery Requirements. The agency shall define and prioritize the requirements to be met before returning an affected or compromised system to normal operations. Recovery strategies may include, but are not limited to:

    - Reinstalling compromised systems from trusted backup-ups; and
    - Reinstalling system user files, startup routines, or settings from trusted versions or sources;

- Validate Restored Systems. Agencies shall validate the restored systems through system or application regression tests, user verification, penetration tests, and vulnerability testing and test result comparisons.

- Increased Security Monitoring. The agency shall heighten awareness and monitoring for a recurrence of the incident.

2.9 Follow-up Analysis

After an incident has been fully handled and all systems are restored to a normal mode of operation, a follow-up analysis should be performed within three to five days of recovering from the incident to discuss actions that were taken and lessons learned. Extended delays may reduce the effectiveness of relating critical information. Follow-up analysis include a review of the chronological events, identifying all containment and eradication actions taken, identification of mitigation strategies, examining the lessons learned, and assessing the incident costs. Questions to be addressed may include, but are not limited to:

- Did detection and response systems work as intended? If not, what methods would have prevented the incident?
- Are there additional procedures that would have improved the ability to detect the incident?
- What improvements to existing procedures and tools would have aided in the response process?
- What improvements would have enhanced the ability to contain the incident?
- What correction procedures would have improved the effectiveness of the recovery process?
- What updates to agency policies and procedures would have allowed the response and recovery processes to operate more smoothly?
- How could user and system administrator preparedness be improved?
- How could communication throughout the detection and response processes be improved?
- Was the incident previously identified as a potential threat?
- What was the impact in terms of financial loss, loss of public or customer trust, legal liability, or harm to public health and welfare?

Results of these questions should be documented and incorporated into existing procedures, if necessary.

2.10 Incident Response Training

2.10.1 All Users

Agencies should provide education and awareness programs for users in incident response procedures and reporting methods. The programs shall address:

Formatted: Font color: Red

Deleted: will

- What types of events are incidents;
- Agency notification procedures; and
- Existing and emerging threats.

2.10.2 Agency IT Staff

Agency staff responding to incidents are encouraged to obtain the following training, according to their roles and responsibilities:

- State and Federal security and privacy laws and procedures
- Technical training on all platforms, operating systems and applications they may be responding to.

2.11 Incident Response Testing

Testing should be conducted at least annually, either in response to an identified incident or as part of a formal readiness test, using defined tests, simulated events, and exercises to determine the effectiveness of the incident response capability.

2.12 Release of Information

Control of information during the course of an incident or investigation of a possible incident is very important. Only the affected agency can authorize the release of all incident information. Specific information concerning the incident, such as accounts involved, programs or system names, are not to be provided to any callers regardless of who they claim to be.

3.0 Applicability

3.1 State Government Agencies

All State agencies, boards, and commissions are required to comply with the standard listed in Section 1.0.

3.2 Exemption

There is no exemption allowed to this Standard by any agency, board, or commission.

4.0 Responsibility

4.1 NITC

The NITC shall be responsible for adopting minimum technical standards, guidelines, and architectures upon recommendation by the technical panel. (Neb. Rev. Stat. § 86-516(6))

4.2 State of Nebraska Information Security Officer

The SISO serves as a security advisor to all State of Nebraska agencies and shall act as the incident response coordinator for the state. In that capacity, the SISO shall perform the following functions:

- Create a statewide incident response reporting procedure and instruct agencies as to the requirements of the procedure.

- Maintain a central list of agency Information Security Officers or incident response point of contact information.

- Receive incident reports, and evaluate, verify, validate and as needed disseminate alerts to State of Nebraska agencies. Alert notification will not include the name of impacted agencies or agency specifics, unless permitted.

- Coordinate with affected agencies in determining the need to disseminate alerts to federal entities, law enforcement, and any other appropriate parties.

4.3 State Agencies

When an incident occurs, agencies must provide a verbal report to the SISO based upon the guidelines listed in section 2.3. A written preliminary report must be completed within two (2) working days using the Incident Reporting Form. This report is to be completed by the individual handling the incident; however all people involved are responsible for providing information regarding their actions. Within ten (10) working days of the resolution of an incident, a written final report must be submitted. In cases where incident resolution is expected to take more than thirty (30) days, a weekly status report must be submitted to the SISO.

Should an incident be serious enough to warrant prosecution, law enforcement will need to demonstrate a chain of custody and provide records of actions taken; therefore a log must be kept, including recovery steps and other regular or routine work performed on the affected system(s). This log should be separate from normal system logs, since it may be used as evidence.

Agencies are responsible for training personnel in incident response capabilities according to their roles and responsibilities.

Agencies that support information systems shall provide a support resource, i.e. a Help Desk, which serves as the primary contact to report incidents.

4.3.1 Agency Incident Response Contacts

Agencies are responsible for providing a primary and secondary point of contact to act as a liaison with the SISO. The agency point of contact can be the agency Information Security Officer (ISO) or some other designee. See Information Security Policy, Appendix B for Roles and Responsibilities of the (ISO).

4.4 Users

All information system(s) users are responsible for understanding their role and complying with agency incident handling procedures. Users must immediately report suspicious activities to their manager and/or agency or State of Nebraska HelpDesk and fully cooperate with personnel tasked with resolving the incident.

5.0 Definitions

Availability. The assurance that information and services are delivered when needed.

Breach. Any illegal penetration or unauthorized access to a computer system that causes damage or has the potential to cause damage.

Chain of Custody. Protection of evidence by each responsible party to ensure against loss, breakage, alteration, or unauthorized handling. Protection also includes properly securing, identifying, and dating evidence.

Compromise. The unauthorized disclosure, modification, substitution, or use of sensitive information, or the successful action to invade system by evading its security. For example, a computer had been compromised when a Trojan horse has been installed.

Confidentiality. The assurance that information is disclosed only to those systems or persons that are intended to received that information.

Continuity of Operations (COOP) Plans – Provides for the continuation of government services in the event of a disaster.

Cyber Security Incident. Any electronic, physical, natural, or social activity that threatens the confidentiality, integrity, or availability of State of Nebraska information systems, or any action that is in violation of the Information Security Policy. For example:

- Any potential violation of Federal or State law, or NITC policies involving State of Nebraska information systems.
- A breach, attempted breach, or other unauthorized access to any State of Nebraska information system originating from either inside the State network or via an outside entity.
- Internet worms, Trojans, viruses, malicious use of system resources, or similar destructive files or services.
- Any action or attempt to utilize, alter, or degrade an information system owned or operated by the State of Nebraska in a manner inconsistent with State policies.
- False identity to gain information or passwords

Denial of Service. An inability to use system resources due to unavailability; for example, when an attacker has disabled a system, or a network worm has saturated network bandwidth.

Incident. An occurrence having actual or potentially adverse effects that causes an interruption of the agency's business activities. It may or may not apply to an Information System.

Incident Response. An organized approach to addressing and managing the aftermath of a security breach or attack (also known as an incident).

Incident Response Team. A group of professionals within an agency trained and chartered to respond to identified information technology incidents.

Information System. A system or application that consists of computer hardware, software, networking equipment, and any data. Such systems include but are not limited to desktop computers, servers, printers, telephones, network infrastructure, E-mail, and web based services.

Integrity. The assurance that information is not changed by accident or through a malicious or otherwise criminal act.

Recovery. A defined step or process within an incident response plan with the goal of returning the affected or compromised systems to normal operations.

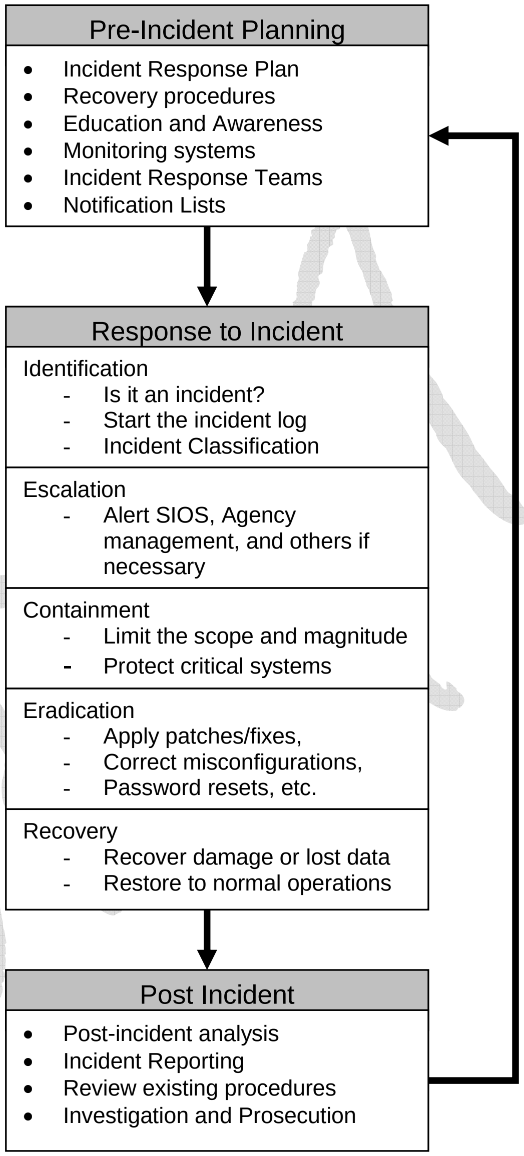
6.0 Related Documents

6.1 NITC Security Officer Handbook (http://www.nitc.state.ne.us/standards/security/so_guide.doc)
6.2 NITC Information Security Policy (http://www.nitc.state.ne.us/standards/index.html)
6.3 State of Nebraska INCIDENT RESPONSE FORM – Attachment A

7.0 References

7.1 National Institute Standards and Technology (NIST) Special Publication, 800-61, “Computer Security Incident handling Guide.” (http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf).

State of Nebraska
Incident Handling Lifecycle



Pre-Incident Planning

- Incident Response Plan
- Recovery procedures
- Education and Awareness
- Monitoring systems
- Incident Response Teams
- Notification Lists

Response to Incident

Identification
- Is it an incident?
- Start the incident log
- Incident Classification

Escalation
- Alert SIOS, Agency management, and others if necessary

Containment
- Limit the scope and magnitude
- Protect critical systems

Eradication
- Apply patches/fixes,
- Correct misconfigurations,
- Password resets, etc.

Recovery
- Recover damage or lost data
- Restore to normal operations

Post Incident

- Post-incident analysis
- Incident Reporting
- Review existing procedures
- Investigation and Prosecution

State of Nebraska INCIDENT RESPONSE FORM

This form is based on the State of Nebraska Incident Response Standard, which agencies are required to use when reporting an incident. An automated version of this form can be found at ??????????. For urgent assistance, contact the State Information Security Officer at (402) 471-7031 or 416-3668.

1. Point of Contact Information for this Incident:

Name:	Agency:
Phone:	Cell/Pager:

2. Physical Location of Affected Computer/Network:

(include building number, room number, etc)

3. Date and Time Incident Occurred and Duration:

(mm/dd/yy)	(hh:mm:ss am/pm)	Duration:

4. Type of Incident (check all that apply):

□ Intrusion
□ Denial of Service
□ Virus / Malicious code (complete 4a)
□ System Misuse
□ Social Engineering
□ Technical Vulnerability (complete 4b)
□ Equipment Missing or Lost (complete 4c)
□ Equipment Stolen or Damaged (complete 4c)

□ Access Control Avoidance
□ Unauthorized Access
□ User Account Compromise
□ Hoax
□ Network Scanning / Probing
□ Root Compromise
□ Web Site Defacement
□ Other (specify)

4a. Provide the name(s) of the virus(es) and any URLs used to obtain information specific to the virus. Provide a synopsis of the incident and any actions taken to disinfect and prevent further infection.

4b. Generally describe the nature and effect of the vulnerability. Describe the conditions under which the vulnerability occurred and the specific impact of the weakness or design deficiency. Has the application vendor been notified?

4c. Provide the make, model, serial number, and tag number:

5. Information on Affected System:

IP Address:	Computer/Host Name:	OS (include release number):	Other Applications:

6. Information on Affected Hardware/Software:

(include version and release information)

7. Number of Host(s) Affected:

□ < 10 □ 10 to 50 □ 50 to 100 □ > 100

8. IP Address of Apparent or Suspected Source:

Source IP Address:	**Other information available:**

9. Incident Assessment:

Is this incident a threat to life, limb, or a critical agency service? □ Yes □ No If yes, elaborate:

List the most restricted classification of the data residing on the system.

Damage or observations resulting from the incident:

10. Information Sharing:

Who can this information be shared with, outside the Office of the CIO? (do not leave blank and check all that apply)

□ Other Agencies □ Law Enforcement ☒ US-CERT □ **No sharing is Authorized**

11. Additional Information:

If this incident is related to a previously reported incident, include previous incident information

Return this form to: State Information Security Officer, 501 S. 14th Street, Lincoln, NE

State Government Efficiency
2008

Objective

- The State Government Council will address multiple items improving efficiency in state government, including implementing shared services and adopting standards and guidelines.

Description

The primary components of this initiative are:

Shared Services. The State Government Council has identified a number of potential shared services. The council chose the following shared services for further study and implementation at this time.

- Business Continuity / Disaster Recovery
- Directory Services
- E-mail
- Enterprise Maintenance / Purchase Agreements
- Geographic Information System (GIS)

Standards and Guidelines. The State Government Council, working with the Technical Panel, will continue to develop standards and guidelines to better coordinate state agency technology efforts.

Benefits

Benefits of this initiative include lower costs, easier interoperability among systems, greater data sharing, higher reliability, and improved services.

Action Plan

Action Items

Shared Services

1. Implement Business Continuity / Disaster Recovery as a shared service.

Action items are included in the Security and Business Resumption initiative.

2. Implement Directory Services as a shared service.

Action items are included in the Security and Business Resumption initiative.

3. Implement E-mail as a shared service.

Lead: Beverlee Bornemeier

Participating Entities: State Government Council, E-mail Work Group

Timeframe: E-mail conversion continues in 2008.

Funding: Service rates

Status: Continuation. As of January 2008, approximately 1,800 state government e-mail accounts have been converted to the Exchange system. Conversion of accounts will continue throughout 2008. Additional actions may include activities relating to records retention for e-mail.

4. Implement Enterprise Maintenance / Purchase Agreements as a shared service.

Lead: Steve Schafer

Participating Entities: State Government Council, EM/PA Work Group

Timeframe: Continuation: Software Reseller Contract Rebid during 2008
New: Others as identified during 2008.

Funding: No funding required.

Status: Ongoing. Master agreements have been established with McAfee, CA, and Symantec for anti-virus and related product suites. Various IBM and Microsoft licenses and maintenance agreements completed for 2008.

5. Implement Geographic Information System (GIS) as a shared service.

Action: NEBRASKA GEOSPATIAL DATA SHARING AND WEB SERVICES

NETWORK. Develop a Nebraska enterprise-level geospatial web portal, with Internet mapping and data services, to serve the users of Nebraska related GIS/geospatial data and enable those users to efficiently and reliably find, access, display, and build public information applications utilizing the geospatial data maintained by a wide variety of state, local and federal agencies and where appropriate, provide for a coordinated security system, including the possibility for limited data access and password protection..

Lead: Larry Zink, Coordinator, Nebraska GIS Steering Committee

Participating Entities: State Government Council; GIS Steering Committee

Timeframe: December 31, 2010 (continuation of earlier action item on Internet Mapping Services)

Funding: A total of $215,000 in grant funding has been secured from the NITC Collaborative Fund, the State Record Board, and the US Geological Survey to underwrite a two-year start up period for this project. An additional $25,000 will be sought from the State Records Board and $60,000 from contributing state agency partners for a total of $300,000. This funding to be supplemented by in-kind technical services provided from state and local agencies.

Status: Continuation. Twelve state and local government agencies have endorsed a Project Charter to indicate their support for, and partnership in, developing this online, enterprise-level GIS/geospatial data mapping and services portal. The bulk of the start up funding is targeted to the hiring of a technical lead for this project. A technical lead recruitment process is currently underway. The project will involve significant technical implementation challenges; including establishing the network, data sharing protocols, and web mapping and data services applications. The technology and system will allow for the live, interactive access and sharing of data from multiple Internet map servers operated by different agencies. The technology will allow agencies to leverage existing state and local investments in data and Internet map services, by other agencies, to build new applications incorporating these Internet map services into their application design. While there is a broad conceptual agreement on the outlines of the desired online network and services, additional planning will be required to define data sharing protocols, data sharing agreements, desired web services, and data access policies.

Action: STREET CENTERLINE-ADDRESS DATABASE. Develop a plan (including responsibilities and resource requirements) for the coordinated development, data integration, on-going maintenance and online distribution/Internet mapping service of a composite, “best available”, statewide street centerline/address database.

Lead: Larry Zink, Coordinator, Nebraska GIS Steering Committee

Participating Entities: State Government Council; GIS Steering Committee

Timeframe: December 31, 2009.

Funding: No enterprise level funding available at this time. However, a grant has been submitted that if successful would provide funding to assist with the development of a business case for the enterprise-level development and maintenance of this database. Major data development funding is on-going through Public Service Commission, Dept. of Roads, and local governments.

Status: Continuation. The Public Service Commission, through the Wireless E911 fund, has worked with counties to contract for the development and maintenance this data for 80 Nebraska counties. The initial data development is complete for least 56 of those 80 counties. For another 27 counties, the initial data development is in process. In addition, Douglas, Lancaster, and Sarpy counties have developed an maintain this data in-house. There are 10 rural counties for which there are currently no active plans for the development of this data. Currently these datasets are maintained in separate county files. The Dept. of Roads maintains geospatial data for all state highways and major local collector roads, but this data does not include street address information. While there are significant public resources being invested in the development of pieces this much needed data, there is currently no plan, or one agency responsible for the on-going collection, integration and distribution of this data in an integrated statewide database format. In 2007, the Office of the CIO and the State Patrol (NSP) cooperated to develop an integrated, “statewide”, street centerline-address files for the 45 counties that were available at that time. This data was needed for the NSP’s new statewide computer-aided dispatch system. The GIS Str. Cmte. has authorized the formation of an Advisory Committee on Street Centerline-Address Databases. That Advisory Committee has begun its work to develop recommendations for an on-going enterprise approach to developing, maintaining, and distributing a statewide, “best available” street centerline-address database from the multiple sources of this data.

Action: METADATA AND STATE GEOSPATIAL DATA CATALOGUE. Document existing state agency GIS/geospatial data with formal metadata and encourage the listing of available geospatial data in Nebraska Geospatial Data Center

Clearinghouse Catalog.

Lead: Larry Zink, Coordinator, Nebraska GIS Steering Committee

Participating Entities: State Government Council; GIS Steering Committee

Timeframe: December 31, 2008.

Funding: Primarily supported through in-kind support of state and local agency personnel

Status: Continuation. The NITC has adopted a Geospatial Metadata Standard (http://www.nitc.state.ne.us/standards/data/metadata_standard_20050923.pdf), which calls for the progressive documentation of state agency geospatial data, within a one-year timeframe (by Sept. 2006). The Department of Natural Resources, in partnership with the Nebraska GIS Steering Committee, has developed a Nebraska Geospatial Data Center (http://www.dnr.state.ne.us/databank/geospatial.html). This Data Center includes a geospatial data clearinghouse and metadata development tools. A two-day metadata training session was held in Lincoln in 2007 and another training session is scheduled for Omaha in 2008. There remains a large body of state agency GIS/geospatial data that has not been documented with metadata and has not been listed on the Data Center Clearinghouse Catalog. The planning Geospatial Data Sharing and Web Services Network will also require metadata document.

Action: STATEWIDE GEOSPATIAL INFRASTRUCTURE STRATEGIC PLANNING. Develop an enterprise-level, statewide, GIS/geospatial infrastructure strategic plan for the geographic area of Nebraska. The planning process should involve the broader GIS user community (state, local, and federal agencies, tribes and the private sector) and seek to identify parallel needs and plans for geospatial data, standards, online distribution networks and services, coordination, funding, and policies.

Lead: Larry Zink, Coordinator, Nebraska GIS Steering Committee

Participating Entities: State Government Council; GIS Steering Committee

Timeframe: June 30, 2009.

Funding: A $50,000 strategic planning grant proposal has been submitted to the Federal Geographic Data Committee (FGDC) by the Office of the CIO on behalf of the Nebraska GIS Steering Committee. If funded, the majority of these grant funds will be used to hire a consultant to assist with this planning process. If not funded, the strategic planning process will still move forward, but on a reduced scale and pace.

Status: New. Over the last 5-6 years, the activities of the Nebraska GIS Steering Committee have been guided by an existing Strategic Plan, the goals of which were originally developed in 2001. The Steering Committee has endorsed a major outreach and planning effort to develop a new GIS/Geospatial Strategic Plan with the goal of facilitating the coordination and collaboration of the broader GIS user community in Nebraska. A grant application has been submitted. A Strategic Planning Advisory Committee has been established to oversee the process and has developed a conceptual outline of the planning process. The GIS Steering Committee, through its Planning Advisory Committee, will lead this process but the active support of the NITC, the State Government Council and its member agencies would be very helpful.

6. Explore requirements for issuing an RFP to contract vendors that provide temporary IT personnel. Meet with participating state agencies to gain input on how to structure and manage a new contract. The current contract originally expired on June 30, 2006 with an option to renew for an additional two years.

Lead: Office of the CIO

Participating Entities: Office of CIO, DAS Materiel Division and state agencies

Timeframe: To be completed by August 2008

Funding: No funding required.

Status: Continuation.

Standards and Guidelines

7. The State Government Council working with the Technical Panel, will continue to develop standards and guidelines to better coordinate state agency technology efforts.

Lead: Rick Becker

Participating Entities: Technical Panel, State Government Council

Timeframe: Ongoing

Funding: None

Status: Ongoing. New and revised standards and guidelines adopted in 2007:

Remote Access Standard, Emergency Information Page, Remote Administration of Internal Devices, Minimum Server Configuration, SMTP Routing Standard, DNS Forwarding Standard, Information Security Policy, Data Security Standard, Password Standard, and Email Policy for State Government Agencies.

Other

8. Review issues and determine process for maintaining an inventory of noneducation state government technology assets, including hardware, applications, and data bases.

Lead: Office of the CIO

Participating Entities: State Government Council

Timeframe: 2008

Funding: None

Status: Continuation.

9. Review issues and determine process for project status reporting.

Lead: Office of the CIO

Participating Entities: State Government Council

Timeframe: 2008

Funding: None

Status: Continuation.

Future Action Items

1. Services identified as potential shared services by the State Government Council include:

Active Directory
Automated Building Systems (HVAC, access, etc.)
Backup Management
Data Network Design
Data Security
Database Management
Desktop Support
Document Management
Electronic Filing
Electronic Records Management
Encryption
Enterprise Knowledge Management Databases
General Platform Management
Help Desk
Instant Messaging
Interactive VRU Applications
Lotus Domino Design and Development
Payment Portal
Project Management
R&D
Remote Access
Secure eFax
Security
Server Consolidation / Virtual Servers
Software Deployment and Management
SQL Database Design and Development
Videoconferencing
Voice Network Design
VoIP
Wireless
Wiring Services
Workflow

Discontinued Action Items

Shared Services

1. Implement Field Support Services as a shared service. The Field Support Services work group is looking for avenues to provide better desktop, server, network, and other Information Technology support to staff outside of the Lincoln area.

Lead: Dale Fangmeier

Participating Entities: State Government Council, Field Support Services Work Group

Status: Discontinued, move to potential shared services list.

Completed Action Items

Other

1. Review and revise procurement review process for IT related purchases by state agencies.

Lead: Steve Schafer

Participating Entities: State Government Council

Status: Completed. Policy developed for NITC approval.

2. Review options for integrating agency IT plans and IT project proposal forms into new budget system.

Lead: Budget Division and Office of the CIO

Participating Entities: State Government Council, Budget Division

Status: Completed. The IT project proposal form has been integrated into the new budget system.

E-Government
2008

Objective

- The State Government Council will continue to implement action items that further the use of e-government to improve services and increase the efficiency and effectiveness of agencies.

Description

The three goals for e-government are:

Government-to-Citizen and Government-to-Business. Anyone needing to do business with state government will be able to go to the state's Web site, easily find the information or service they need, and if they desire, complete all appropriate transactions electronically. Areas to be addressed include citizen portal enhancement; business portal enhancements; education portal; and forms automation.

Government-to-Government. State agencies will improve services and increase the efficiency and effectiveness of government operations through collaboration, communication, and data sharing between government agencies at all levels.

Government-to-Employee and Internal Operations. Agencies will examine internal operations to determine cost-effective e-government applications and solutions. The purpose of these efforts is to improve efficiency and effectiveness by replacing manual operations with automated techniques.

The e-government principles guiding the council are:

- E-government should be considered a continuous process of using technology to serve citizens and improve agency operations;
- Internet technologies create new opportunities for major change, including self-service, integration of information and services, and elimination of time, distance and availability of staff as constraints to providing information and services;
- Agencies have responsibility for performing statutory functions, which means that

agency directors must retain ownership of data, responsibility over the use of information technology, and prioritization of projects within the agency to achieve the greatest benefit;

- Cooperation is critical to achieving the goals of e-government, in order to integrate information and services and allow the easy exchange of information;
- An enterprise approach is essential to e-government, including the topics of accessibility for disabled persons, architecture, directories, funding, portal, privacy, security, and other issues; and
- E-government is defined as the use of technology to enhance information sharing, service delivery, constituency and client participation, and governance by transforming internal and external relationships.

Benefits

The primary benefits from the use of e-government are:

- Improved services for citizens and businesses.
- Increased efficiency and effectiveness for agencies.

Action Plan

Action Items

1. Work with the various agencies involved in business registration—including the Secretary of State, Department of Revenue, and Department of Labor — to create an online system for business registration.

Lead: Nebraska.gov

Participating Entities: State Government Council, Nebraska.gov, agencies

Timeframe: 2008

Funding: To be determined.

Status: Continuation. Phase 1 of this action item was completed in November 2007 with the creation of the Nebraska One-Stop Business Registration Information System website (https://www.nebraska.gov/osbr/).

Future Action Items

1. Work with the Nebraska.gov Manager and county officials to provide the means for online payment of property taxes and other local fees. This system is currently being provided by NACO/MIPS. Nebraska.gov will consider the cost benefit of moving forward with this project.

2. Work with the Nebraska State Patrol to review options for providing online access to certain, limited, criminal history information.

3. Develop an online application for use by businesses attempting to find a suitable site for business development.

4. Develop strategies to address the following government-to-government activities:

- Intergovernmental Cooperation Groups. Expand upon current intergovernmental cooperative efforts like the CJIS Advisory Committee and GIS Steering Committee; and develop new cooperative groups for those agencies that have specific, shared interests.

- Integration of Government Information and Services. Develop strategies for using Internet technologies to provide integrated access to information and services to citizens, businesses, employees, and other governmental entities.

- Forms Automation. Work with state agencies and political subdivisions to identify and prioritize opportunities for automating forms that local government uses to interact with state government.

5. The State Government Council will identify specific improvements and value-added services to be incorporated into the state employee portal.

6. Develop method of providing authentication for “first time” users.

7. Work with the Department of Motor Vehicles to provide for online specialty plate ordering and vehicle registration.

Discontinued Action Items

1. Convene a work group to examine opportunities to improve access to information resources through a knowledge management system.

Lead: Office of the NITC

Participating Entities: Community Council, Education Council, State

Government Council, Technical Panel, and Nebraska.gov

Status: Discontinued

Security and Business Resumption
2008

Objective

- This initiative will define and clarify policies, standards and guidelines, and responsibilities related to the security of the state's information technology resources.

Description

Information security will serve statutory goals pertaining to government operations and public records. These include:

- Insure continuity of government operations (Article III, Section 29 of the Nebraska Constitution; Nebraska Revised Statutes Sections 28-901 and 84-1201);
- Protect safety and integrity of public records (Nebraska Revised Sections 28-911, 29-2391, and 84-1201);
- Prevent unauthorized access to public records (Nebraska Revised Statutes Sections 29-319, 81-1117.02, and 84-712.02);
- Insure proper use of communications facilities (Nebraska Revised Statutes Section 81-1117.02); and
- Protect privacy of citizens (Nebraska Revised Statutes Section 84, Article 7).

Major activities include:

- Developing an overall security strategy, including policies, security awareness, and security infrastructure improvements;
- Network security standards and guidelines;
- Education and training;
- Authentication (directory services project);
- Disaster recovery for information technology systems (as part of a broader business continuity planning);

- Compliance with federal privacy and security mandates;
- Security assessments.

Benefits

Benefits will include lower costs by addressing security from an enterprise perspective, cost avoidance, and protecting the public trust.

Action Plan

Action Items

Security

1. Implement security incident response team.

Lead: State Security Officer and State Patrol

Participating Entities: State Government Council, Security Work Group

Timeframe: Spring / summer 2008

Funding: No funding required for this task.

Status: Continuation

2. Enhance Network Security and Network Management.

Action: Evaluate and recommend options for a Network Operation Center that will provide real-time monitoring of all critical assets within the State of Nebraska.

Lead: Office of the CIO - Wide Area Network

Participating Entities: State Government Council

Timeframe: 2008

Funding: Homeland Security Grant funding / Additional funding has yet to be determined.

Status: New

Business Resumption

3. Implement shared disaster recovery facilities. Mission critical systems have three common requirements. Recovery times must be measured in hours, not days or weeks. Recovery facilities should be physically separated so that they will not be affected by a single disaster. There must be staff available to assist with the recovery efforts. Achieving these requirements is very expensive. Sharing disaster recovery facilities and establishing a collaborative approach to disaster recovery is one strategy for managing costs. The Office of the CIO and the University of Nebraska are jointly developing a fast recovery capability using mutual assistance of physically separated data centers.

Lead: Office of the CIO and University of Nebraska

Participating Entities: State Government Council

Timeframe: Ongoing

Funding: The cost and source of funding have not been determined.

Status: Continuation. An alternate site providing greater geographical separation has been selected. In the pursuit of establishing that alternate site, the University of Nebraska and the Office of the CIO are reviewing vendor RFP responses and are preparing to act on two important items:

- Establishing the fiber optic communications link between the University and State enterprise server primary sites located in Lincoln and an alternate site that provides greater geographic separation.

- Acquiring and implementing an enterprise server that can provide backup and execute assigned processing loads

The intent is to complete the acquisition/implementation of both items in the next year. When completed, the University and the State will not only have their critical data mirrored at a geographically separated site, but will have the capability at the alternate site to continue the most critical enterprise server production processing with less than 10 hours interruption.

4. Promote disaster planning for information technology systems, including developing elements of a common planning document and developing an approach for common governance during an event.

Lead: Steve Henderson / Dave Berkland

Participating Entities: State Government Council

Timeframe: Ongoing

Funding: No funding required.

Status: Continuation. The Director-level meetings, chaired by Lt. Governor Sheehy, identified critical business functions and categorized them into one of three categories: public safety, public health and institutional care. Progress has been made with public safety (lead by Nebraska State Patrol) in identifying:

- the agencies that work together in the public safety domain
- the data the partners use to complete their work
- the IT infrastructure used to support the data

Initial kick-off meetings have been held with public health (lead by Department of Health and Human Services) to identify the same items. Work continues with Nebraska Emergency Management Agency to understand and refine the implementation of the incident command system and its interactions with the State EOC. Work to integrate continuity of operations, disaster recovery, emergency operations and emergency action plans has begun.

Completed Action Items

Security

1. Conduct annual independent security audits. Multiple federal programs require periodic computer security audits, including HIPAA, HAVA, and Bioterrorism grants from the Center for Disease Control. Computer security audits are a widely accepted best practice across the public and private sector.

Lead: State Security Officer

Participating Entities: State Government Council, Security Work Group

Timeframe: Implementation timeframe is March/April 2008.

Funding: Government Technology Collaboration Fund.

Status: Completed. An RFP was awarded Feb. 7, 2008 to IBM to implement the Qualys solution on 2600 devices.

2. Enhance Network Security and Network Management. (New action items listed above, completed action items listed here.)

Action: Investigate and recommend an enterprise solution to ensure that encrypted traffic adheres to State security requirements.

Lead: Office of the CIO - Network Support

Participating Entities: State Government Council

Timeframe: Feb. 2008

Funding: No funding required for this task.

Status: Completed with the migration of all Avaya firewalls to the Fortinet infrastructure.

Action: Evaluate and recommend options for providing encryption to clients across the state's Wide Area Network.

Lead: Office of the CIO - Wide Area Network

Participating Entities: State Government Council

Timeframe: March 2008

Funding: No funding required for this task.

Status: Completed. The State of Nebraska has entered into a Contract with PGP for whole disk encryption.

Action: Evaluate and recommend options for providing compliance auditing across the state's Wide Area Network.

Lead: State Security Officer and Office of the CIO - Wide Area Network

Participating Entities: State Government Council

Timeframe: 1st Qtr 2008

Funding: No funding required for this task.

Status: Completed**.** The State of Nebraska has purchased Cisco's Compliance Manager and has been attending training classes for staff.

Business Resumption

3. Encourage testing and updating of disaster plans.

Lead: Steve Henderson / Dave Berkland

Participating Entities: State Government Council

Timeframe: Ongoing

Funding: No funding required.

Status: Completed. The Continuity of Operations Planning/Disaster Recovery Planning Shared Services Group worked to develop and act on ways to better coordinate disaster recovery planning and to provide for more consistent disaster recovery plans. An NITC standard ("Information Technology Disaster Recovery Plan Standard") has been put in place. Work has been completed to better understand disaster recovery plan assumptions and dependencies.

Future Action Items

1. Convene a work group to improve disaster recovery and business continuity procedures, including homeland security preparedness, for all public entities.