Approved: April 30, 2003
Date

MINUTES OF THE SELECT COMMITTEE ON KANSAS SECURITY

The meeting was called to order by Chairperson Lee Tafanelli at 1:00 a.m. on April 4, 2003 in Room 519-S of the Capitol.

All members were present except:	Representative Carl Krehbiel - Excused Representative John Faber - Excused Representative Judy Showalter - Excused Representative Tom Holland - Excused Representative Andrew Howell - Excused
Committee staff present:	Robert Waller, Legislative Research Department Bruce Kinzie, Office of the Revisor of Statutes Carol Doel, Committee Secretary
Conferees appearing before the committee:	Bruce Roberts, Chief Information Technology Officer, Executive Branch Don Heiman, National Association of State Chief Information Officers
Others attending:	See attached sheet

Having addressed the other elements of security, Chairman Tafanelli introduced Bruce Roberts Chief Information Technology Office, Executive Branch to brief the committee on information technology and information security. During 2002 they worked closely with a sub-committee of the ITAB (Information Technology Advisory Board to develop a draft policy for ITEC establishing an enterprise IT Security Council. They appointed Larry Kettlewell in the Kansas Information Technology Officer to be the Kansas Chief Information Security Office and he co-chairs the council with Tim Blevins Chief Information Officer, Kansas Department of Revenue. The Council has members from 13 State agencies and representation of the Information Network of Kansas, the US Secret Service, and county government.

Mr. Roberts included in his presentation the Kansas IT Governmental Model primarily to show the committee the box that represents the Security Council which is right in the center of the diagram. He also related some of the issues which the council dealt with such as reviewing other state legislation for open records exemption for IT security information. They also prepared some draft legislation which has not yet been introduced, but is being held for possible serious consideration for next year. The Security Council meets monthly and spend quite a few of their meetings reviewing strategies and software tools to assist with the enterprise risk analysis and assessment. They have also established regular meetings and try to improve the coordination with the Homeland Security elements both federally and here in the State. The Council is looking at incident reporting and considering, also, if our current statutes is appropriate to deal with potential criminal prosecution of infractions. Finally they recognize, as they have come together and formed an important part of the government's model, that we need to increase our commitment to a true addressing of enterprise security operationally for IT. Mr. Roberts also addressed the management recommendations, technology, operational assessment, telecommunications infrastructure as well as the importance of staffing enterprise security adequately to protect the state's infrastructure. (Attachment 1)

Next to address the committee was Don Heiman of National Association of State Chief Information Officers (NASCIO). Mr. Heiman recently retired from the State of Kansas, where he served four years as the chief information technology officer for the executive branch and chief information technology architect for the three branches of government as well as having served in several other Kansas state agencies. Mr. Heiman chaired the National Committee on Security during the time of 9-11.

NASCIO asked Mr. Heiman to draft a national call to action for the federal government and state governments. This was funded by PricewaterhouseCoopers endowment for the business of government. A copy of this draft was supplied to each member of the committee. It is entitled *Public-Sector Information Security: A Call to Action for Public-Sector CIOs.*

This booklet covered recommendations, a report from the NASCIO forum on security and critical

Unless specifically noted, the individual remarks recorded herein have not been transcribed verbatim. Individual remarks as reported herein have not been submitted to the individuals appearing before the committee for editing or corrections.

infrastructure protection and also listed the names of the forum participants. (A copy of this booket may be obtained or viewed by contacting:

Mr. Chris Dixon
NASCIO
167 West Main Street, Suite 600
Lexington, KY 40507-1324
or e-mail: nascio@amrinc.net)

Mr. Heinen stressed the importance of cooperation between information, telecommunications, banking and finance, government, government sources, transportation and energy.

With no further business before the committee, Chair Tafanelli adjourned the meeting at 2:00 p.m.

SELECT COMMITTEE ON KANSAS SECURITY

GUEST LIST

Date 4/4/03

Rick Miller, 296-2271 KITO	
Carl Holmes	

Data and Telecommunications Security Update
Testimony Before House Select Committee on Kansas Security
Bruce Roberts
Chief Information Technology Officer, Executive Branch

April 4, 2003

Introduction

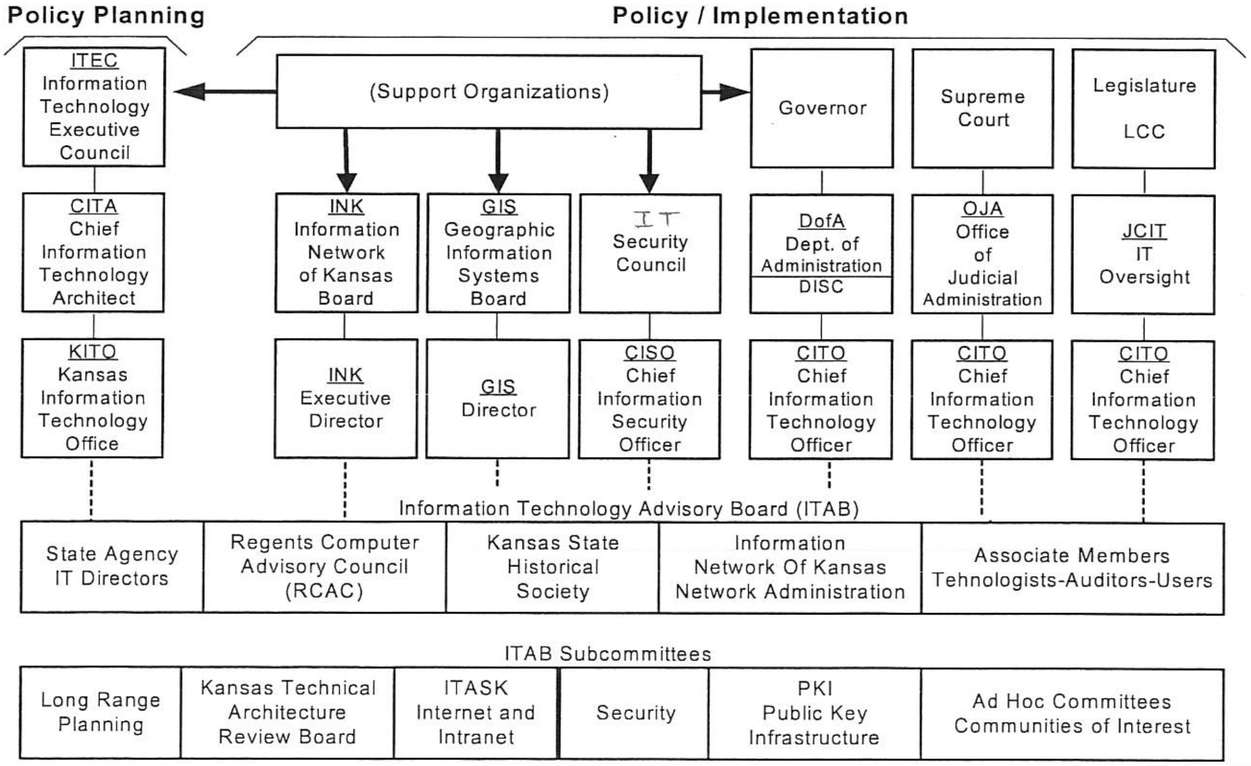
Mr. Chairman and members of the committee. My name is Bruce Roberts and I serve as the Chief Information Technology Officer for the Executive Branch.

Thank you for the opportunity to provide information to you about the state of IT security for Kansas government's telecommunications and data infrastructure. My goal is to provide you with updates on our activities and accomplishments over the last year and to explain some of the initiatives underway for addressing security issues in the future.

Establishing the Enterprise Security Council

During 2002 we worked closely with a sub-committee of the Information Technology Advisory Board (ITAB) to develop a draft policy for ITEC establishing an enterprise IT Security Council. ITEC adopted the policy at its April 2002 meeting. We appointed Larry Kettlewell in the Kansas Information Technology Office to be Kansas Chief Information Security Officer and he co-chairs the council with Tim Blevins, Chief Information Officer, Kansas Department of Revenue. The Council has members from 13 state agencies and representation of the Information Network of Kansas, the US Secret Service, and county government.

Kansas IT Governance Model


Policy Planning
Policy / Implementation
ITEC Information Technology Executive Council
(Support Organizations)
Governor
Supreme Court
Legislature LCC
CITA Chief Information Technology Architect
INK Information Network of Kansas Board
GIS Geographic Information Systems Board
IT Security Council
DofA Dept. of Administration DISC
OJA Office of Judicial Administration
JCIT IT Oversight
KITO Kansas Information Technology Office
INK Executive Director
GIS Director
CISO Chief Information Security Officer
CITO Chief Information Technology Officer
CITO Chief Information Technology Officer
CITO Chief Information Technology Officer
Information Technology Advisory Board (ITAB)
State Agency IT Directors
Regents Computer Advisory Council (RCAC)
Kansas State Historical Society
Information Network Of Kansas Network Administration
Associate Members Tehnologists-Auditors-Users
ITAB Subcommittees
Long Range Planning
Kansas Technical Architecture Review Board
ITASK Internet and Intranet
Security
PKI Public Key Infrastructure
Ad Hoc Committees Communities of Interest

SELECT COMMITTEE ON
KANSAS SECURITY
Attachment 1
Date 4-4-03

- ITEC Policy 4300 (attached)
- Membership (attached), council meets monthly.
- Establishing the council enhances the Kansas IT Governance Model by formalizing a critical support organization to develop and implement effective policies, procedures, and practices for IT security.

Security Council's Initial Focus (1st Nine Months)

- IT Security Exemption from Open Records Laws - draft legislation (attached)
- Enterprise Risk Analysis/Assessment
- IT Security Coordination including Homeland Security
- Incident reporting and criminal prosecution
- Developing an Enterprise Virtual Security Office

Ten Recommendations Frame the Council's Work

Public-Sector Information Security: A Call to Action for Public-Sector CIOs
Prepared by Don Heiman, former CITO, Kansas Executive Branch, July 2002
Sponsored by The PricewaterhouseCoopers Endowment for The Business of Government
http://www.endowment.pwcglobal.com/pdfs/HeimanReport.pdf

Management Recommendations

1. Make sure that everyone is at the table. Creating the IT Security Council has helped us formalize enterprise coordination and to raise awareness and commitment of stakeholders.
2. Develop measures for enterprise success....planning for security outcomes, best practices, and information sharing
   a. Kansas Statewide Information Technology Architecture
   b. ITEC Policy on Agency Security Policies
   c. Incident metrics through Intrusion Detection System
   d. The Technical User's Group, ITAB Security Subcommittee
   e. Participate in Kansas Public Safety Communications Committee
3. Adopt IT control objectives to manage, implement, and maintain IT systems.
   a. Kansas has adopted the Control Objectives for IT (COBIT) standards.
   b. ISO 17799 - a comprehensive set of controls comprising best practices in information security
   c. Federal Information Systems Control Audit Manual (FISCAM)
4. Develop security metrics...for intrusions, security breaches, penetrations, and vulnerabilities. Report metrics at a summary level.
   a. ISS Real Secure reports on the status of KANWIN and D of A DMZ
   b. System log analysis (SYSLOG)

5. Develop state enterprise-IT architectures that include security as an underlying domain.

    a. Kansas Statewide IT Architecture release 10.0 in July 2003
    b. Security chapter – Wireless on the horizon
    c. Common architecture for Geographic Information Systems

6. Develop a business case for security based on a full risk assessment of critical-infrastructure vulnerabilities.

    a. The Security Council is planning for this assessment.
    b. The Security Council is also in the process of identifying the top 10 applications for vulnerability assessment.

Technology Recommendations

7. Deploy automated and manual security technologies based on asset inventories.

    a. ISS Real Secure Intrusion Detection
    b. Honey Pots - Set up to display vulnerabilities cues counter actions
    c. Scanners - LanGuard, Ethereal, Nessus

    We are also currently reviewing automated enterprise asset management solutions

    Internet Security Systems (ISS) Dynamic Threat Protection
    Archer Technologies Security 2002
    Bindview

8. Develop a state security portal …Private and Public

    a. KDEM has requested Private portal and we are working with them to develop
    b. The public portal is an extremely important part of the national plan and we expect that there will be federal funding made available to the states for educational programs.

    Home users
    Cable and DSL "always on" technology is both a blessing and a curse. Home users are "appliance operators" often with no anti-virus software and or firewalls, which increases risks for acting as continuing infecting agents and increases vulnerability to data, identity and credit card theft.

Homeland Security

9. Establish an interstate security information sharing and analysis center (interstate ISAC).

    This is an initiative that the National Association of State Chief Information Officers (NASCIO) has actively pursued during the last two years. Federal funding has not yet occurred (nationally need is estimated at $25M, with approximately $750,000 allocated to Kansas).
    States have taken the lead (especially Kansas) in advocating an Interstate ISAC. The center will coordinate the dissemination of cybersecurity information from the

Department of Homeland Security and coordinate information among the states, with each state serving as a collection point for threats within their state and as a dissemination point for entities in their state (state agencies, educational entities, county and city government). NASCIO has just distributed the formal agreements to the states for consideration and execution and is coordinating funding requests with congress.

10. Develop model state legislation for confidential sharing of information.

    Security Council IT security exemption from open records

    Federal legislation forthcoming as an umbrella to modify the Freedom of Information Act relative to cybersecurity.

Operational Assessment

Our early experience with Real Secure (IDS monitoring software) is that we have additional work to do to secure all state network subscribers. We are analyzing the last quarters' data and adjusting the monitoring parameters to identify vulnerabilities more efficiently. These metrics combined with a statewide asset inventory and risk assessment will continue to reduce vulnerabilities associated with configuration problems of IT assets and protect other network devices from viruses and other cyber attacks. We continue to emphasize good security practices to the agencies to keep security patches current and to ensure that virus protection is installed and current.

Telecommunications Infrastructure

DISC is in the process of improving the state's data network survivability by establishing a network node at the Historical Society. This facility is expected to operational by August and will enhance the business continuity of state agencies connected to the network, especially those operating within the capitol complex.

Virtual Security Office

Recognizing the importance of staffing enterprise security adequately to protect the state's infrastructure, the Security Council has been developing a concept of a "virtual" enterprise security office. This effort would call upon state agencies to share staff and expertise to contribute to monitoring, reporting, and correction of security issues throughout the enterprise. Given the current fiscal crisis, we believe that by joining together, we can still make significant progress toward information technology security goals. Clearly, if federal funding comes about, it would help significantly with this effort.

I will be glad to stand for questions.

The State of Kansas
Information Technology Executive Council

Information Technology Policy #4300 Revision #0

1.0 TITLE: Information Technology Security Council Charter

1.1 EFFECTIVE DATE: 02 May 2002.

1.2 TYPE OF ACTION: New.

2.0 PURPOSE: To establish an Information Technology Security Council that is advisory to the Information Technology Executive Council (ITEC).

3.0 ORGANIZATIONS AFFECTED: All divisions, departments, agencies, boards and commissions of the state.

4.0 REFERENCES:

4.1 K.S.A. 1998 Supp. 75-7203 authorizes the ITEC to: Adopt information resource policies and procedures and provide direction and coordination for the application of the state's information technology resources for all state agencies.

5.0 DEFINITIONS:

5.1 Information technology is an inclusive term to address the services and functions commonly associated with information systems and telecommunications.

6.0 POLICY:

6.1 The Information Technology Security Council shall:

6.1.1 Address information technology security issues and provide policy, standards, guidelines, or procedural recommendations to the Information Technology Executive Council;

6.1.2 Initiate and recommend security specifications for statewide contracts for common information technology requirements from suppliers qualified by the Division of Purchases.

6.1.3 Review proposed programs and projects referred by Chief Information Technology Officers and make recommendations regarding the appropriateness of security measures, technologies used, compliance with policy and standards, conformity with the Kansas State Technical Architecture and resource estimates;

6.1.4 Provide guidance to the Kansas State Technical Architecture Security Subcommittee regarding security aspects of the architecture

6.1.5 Contribute to and support the Strategic Information Management Plan and the annual Information Technology Plan;

6.1.6 Promote coordination and cooperation among state organizations' for effective integration and use of information technology security;

6.1.7 Promote and coordinate Quality Assurance of IT security processes and practices;

6.1.8 Promote and coordinate IT security audits throughout the enterprise.

6.1.9 Address information technology security resource management issues at the request of the ITEC and make recommendations thereon.

7.0 PROCEDURES:

7.1 The Security Council shall be composed of the following members:

7.1.1 A representative from the Kansas Adjutant General's Department

7.1.2 A representative from the Department of Administration

7.1.3 A representative from the Kansas Department of Agriculture

7.1.4 A representative from the Office of the Kansas Attorney General

7.1.5 A representative from the Kansas Department of Corrections

7.1.6 A representative from Federal Law Enforcement [as *ex officio member*]

7.1.7 A representative appointed by the Kansas Chapter, Association of Government Management Information Sciences

7.1.8 A representative from the Kansas Department of Health and Environment

7.1.9 The Executive Director of the Information Network Kansas

7.1.10 A representative from the Kansas Bureau of Investigation

7.1.11 A representative from the Judicial Branch

7.1.12 A representative from the Kansas Juvenile Justice Authority

7.1.13 A representative from the Kansas Legislative Post Audit

7.1.14 A representative from the Kansas Board of Regents

7.1.15 A representative from the Kansas Department of Revenue

7.1.16 A representative from the Kansas Social and Rehabilitation Services

7.1.17 A representative from the Kansas Department of Transportation

7.2 Each organization specified in section 7.1 shall appoint as their representative to the Information Technology Security Council, the person most qualified to discharge the intent of this charter. The ITEC or the Information Technology Security Council may seek representation from additional state agencies to serve as voting members. Additional local, state, federal and private sector members may participate as deemed appropriate by the Security Council.

7.3 The organizations specified in section 7.1 shall notify the Kansas Information Technology office of their designated representative for service on the Security Council.

7.4 For administrative purposes, the Information Technology Security Council will receive staff support from the Kansas Information Technology Office.

8.0 RESPONSIBILITIES:

8.1 The Kansas Information Technology Office is responsible for the maintenance of this policy.

9.0 CANCELLATION: None

10.0 CONTACT PERSON: Kansas Information Technology Office, 785-296-3463

Kansas Information Technology Security Council
Membership

In accordance with paragraph 7 of Information Technology Executive Council policy #4300, the following representatives have been nominated to represent their agencies or departments on the Kansas Information Technology Security Council:

Kansas Adjutant Generals Department – Colonel Henry Martin

Kansas Department of Administration – Eldon Rightmeier, DISC

Kansas Department of Agriculture – Hank Sipple

Office of the Kansas Attorney General – vacant

Kansas Department of Corrections – Norman Bacon (acting)

Federal Law Enforcement representative - Ian Benny, US Secret Service *(ex officio member)**

Kansas Chapter, Association of Government Management Information Services – Jim Lawson, Douglas County

Kansas Department of Health and Environment – Dean O'Brian

Executive Director, Information Network Kansas – Jim Hollingsworth

Kansas Bureau of Investigation – Ron Rohrer

Kansas Judicial Branch – Doug Cruce

Kansas Juvenile Justice Authority – Todd Reinert

Kansas Legislative Post Audit – Allan Foster*

Kansas Board of Regents – Chuck Crawford

Kansas Department of Revenue – Tim Blevins, Co-chair
(Stan Weichert – alternate member)

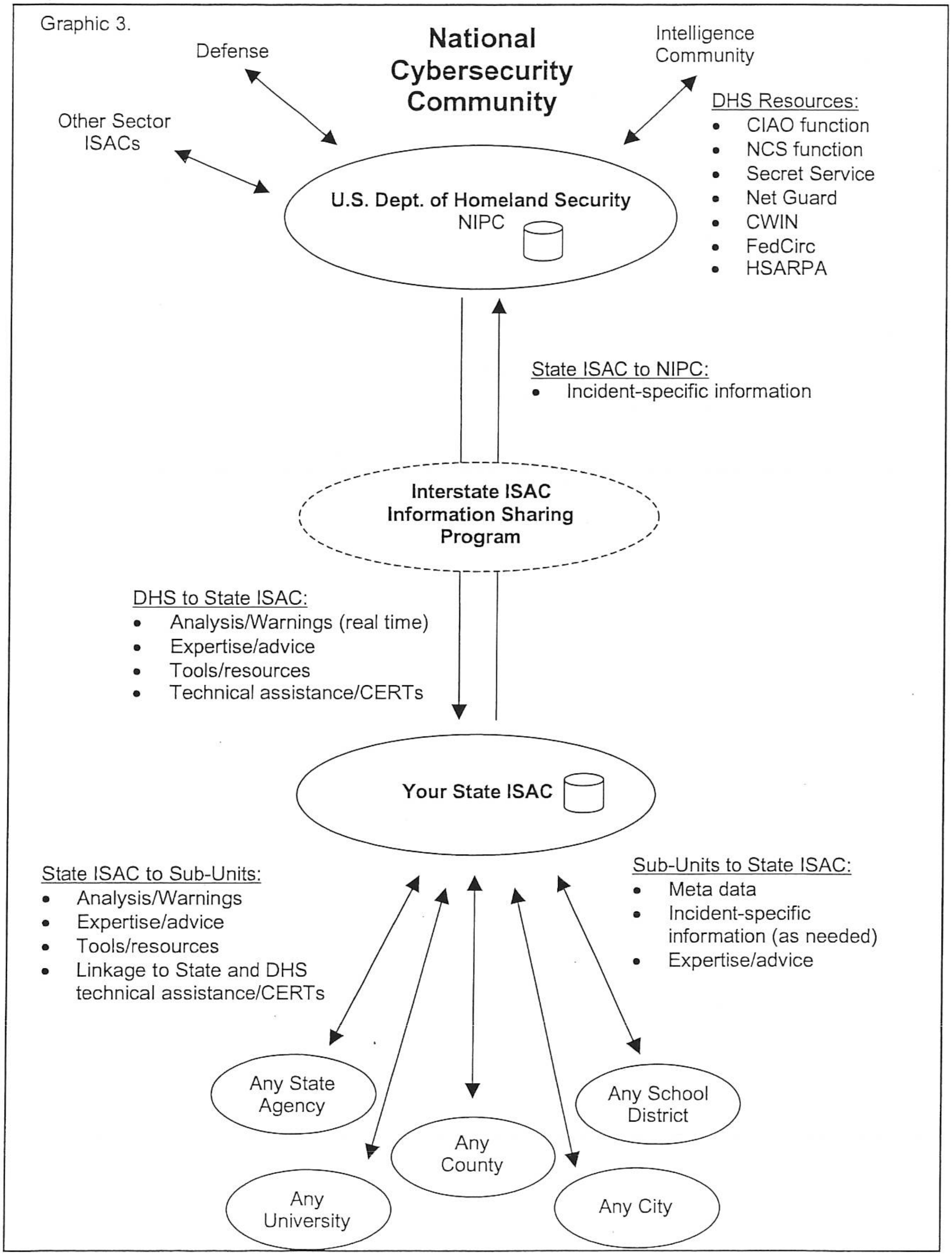
Kansas Social and Rehabilitation Services – Carol Stuckey

Kansas Department of Transportation – Ben Nelson

Kansas Information Technology Office – Larry Kettlewell, Co-chair

* denotes non-voting member

Graphic 3.



DHS Resources:

- CIAO function
- NCS function
- Secret Service
- Net Guard
- CWIN
- FedCirc
- HSARPA

State ISAC to NIPC:

- Incident-specific information

DHS to State ISAC:

- Analysis/Warnings (real time)
- Expertise/advice
- Tools/resources
- Technical assistance/CERTs

State ISAC to Sub-Units:

- Analysis/Warnings
- Expertise/advice
- Tools/resources
- Linkage to State and DHS technical assistance/CERTs

Sub-Units to State ISAC:

- Meta data
- Incident-specific information (as needed)
- Expertise/advice

Proposed Change to Open Records Act
Final Version
As passed by the Kansas Information Technology Security Council
Tuesday, October 15, 2002

(x) Records jeopardizing the security of electronic information processing systems, telecommunications systems or other communications systems of or used by a public agency including:

a) Plans, diagrams, security codes, user ids, passwords, combinations, or computer software and hardware including logs produced therein; used to protect electronic information and government property;

b) Information that would identify those areas of structural or operational vulnerability that would permit unlawful disruption to, or interference with, the services provided by a public agency; and

c) Information that could be used to disrupt, interfere with, or gain unauthorized access to electronic information or government property.