

# Threat Information and Infrastructure Protection Program (TIIPP)



Located within DPS Intel Div/Fusion Center



# HISTORY OF HOMELAND SECURITY

# History of Homeland Security



- 9/11 attacks were a watershed for U.S. emergency management policy
- Federal response passed Homeland Security Act of 2002
  - Created the U.S. Department of Homeland Security (DHS) in 2003
  - Absorbed FEMA and many other agencies
- Since that time, there has been a national struggle in defining what the term really means



# History of Homeland Security - Iowa

- HS coordination function located within Iowa Emergency Management Division (renamed the Iowa Homeland Security and Emergency Management Division) of the Iowa Department of Public Defense soon after September 11<sup>th</sup>, 2001
- Important to note that as in emergency management, HSEMD's role in homeland security is mainly in coordination, not implementation
- Agencies such as DPS, IDOT, IDPH, IDALS etc. each have important roles to play in the process
- HSEMD coordinates all these roles into one functional homeland security program

# History of Iowa Homeland Security (HS)



- Beginning in 2003, HSEMD stood up a HS Bureau that focused on HS strategic planning, HS program management and other duties as assigned
  - Coordinates first responders, state agency directors and key players, working together to increase security in Iowa
  - Incorporated work in asset protection, infrastructure protection, information sharing and grants management
  - Manages and coordinates multi-discipline projects from critical infrastructure protection to public/private partnership, from strategic planning to grants policy management, from management of the clearance process to OPSEC



# ROLES AND RESPONSIBILITIES

# Homeland Security Team



- Curt Sullivan – Asset Protection Planner
- Vacant – Infrastructure Protection Planner
- Brian Lewis – Information Security Officer

# The Asset Protection Planner



- Focuses primarily on the identification and protection of individual assets within the State of Iowa
- Supplements Sector Planning by contributing asset identification criteria for each sector
- Works as the individual asset holders voice in the fusion center process [Fusion Center Baseline Capability I.A.9]
- In addition to interfacing with the assets themselves and providing technical assistance on protective measures and vulnerability assessments, the Asset Planner administers the Buffer Zone Protection Program and the Automated Critical Asset Management System
- Trained in Vulnerability Assessment Methodologies
- PClI officer for the State of Iowa



# The Infrastructure Protection Planner



- Focuses on developing relationships within and between Iowa's critical infrastructure sectors, and using these relationships to identify sector and cross-sector interdependencies
- Writes Iowa Sector Reference Documents
- Primarily responsible for the interface between HSEMD, the different critical infrastructure sectors in Iowa, and cross-sector groups such as the Safeguard Iowa Partnership
- Provides technical assistance on protective measures and vulnerability assessments through the sector leads, and points of contact
- Public Private Partnership [P3] integration into the Iowa Fusion Center, acting as the sector level points of contact voice in the fusion center process [Fusion Center Baseline Capability I.A.9]
- Assists the Asset Protection Specialist in the implementation and use of ACAMS (Assistant Trainer)
- Trained in Vulnerability Assessment Methodologies
- Deputy PClI Officer for the State

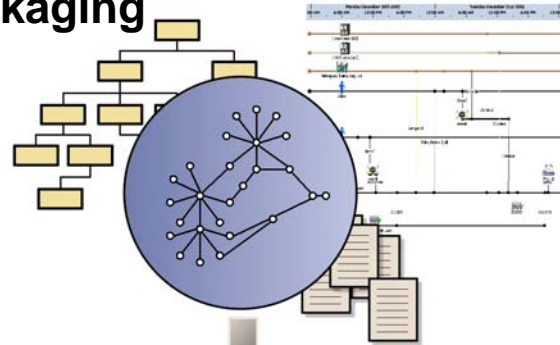
# The Information Security Officer (ISO)



- Primarily responsible for the administration of the information sharing components of Iowa's critical infrastructure programs
- Provides information security technical support and manages Iowa's OPSEC program
- Responsible for maintaining the State of Iowa Homeland Security Advisory System, facilitating the "special events" coordination activities of the Division and security clearance maintenance
- Administers Homeland Security Information Network (HSIN) conduit of secure information flow to the sector and asset points of contact. (Public and Private partnership on information sharing process)
- Weekly TIIPP report

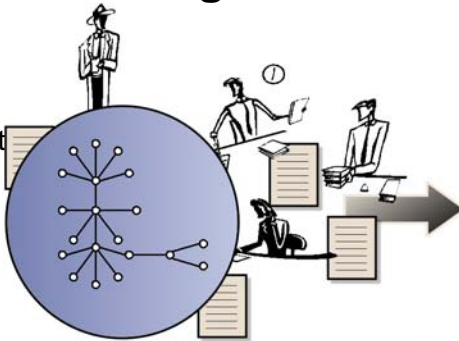
# TIIPP Overview

## Information Collection & Packaging



## Preparedness Planning

- Threat Assessment
- BZPP
- Special Event Security
- Site Assessments
- Sector Planning
- ACAMS



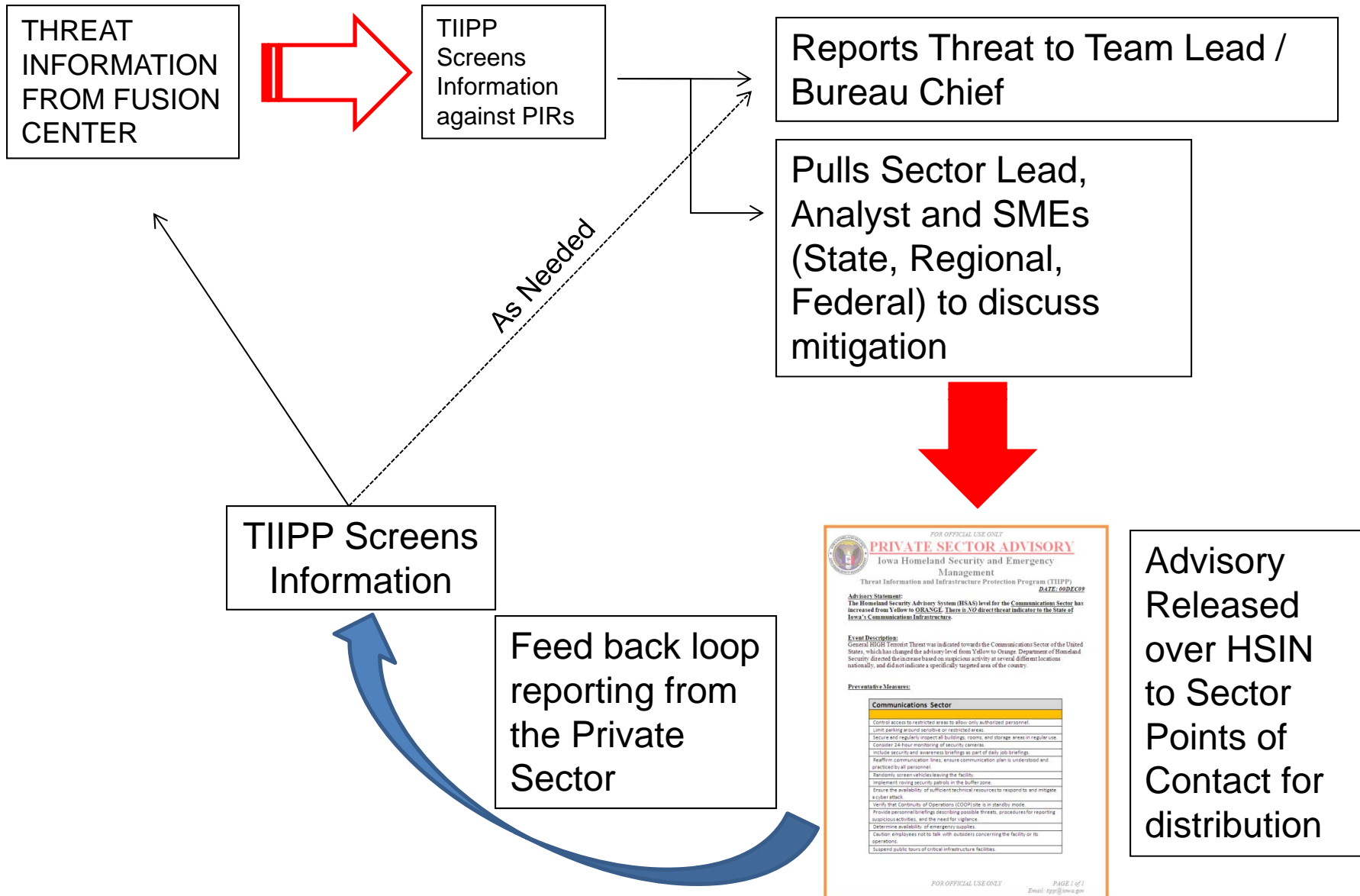
## Threat Analysis & Reports/Alerts



## Training



# TIIPP Overview (Threat information Process)



FOR OFFICIAL USE ONLY

**PRIVATE SECTOR ADVISORY**  
Iowa Homeland Security and Emergency Management  
Threat Information and Infrastructure Protection Program (TIIPP)  
ZUIZE-00000009

**Advisory Statement:**  
The Homeland Security Advisory System (HSAS) level for the Communications Sector has increased from Yellow to ORANGE. There is NO direct threat indicator to the State of Iowa's Communications Infrastructure.

**Event Description:**  
General HIGH Terminate Threat was indicated towards the Communications Sector of the United States, which has changed the advisory level of Iowa Yellow to Orange. Department of Homeland Security directed the increase based on suspicious activity at several different locations nationally, and did not indicate a specifically targeted area of the country.

**Preventative Measures:**

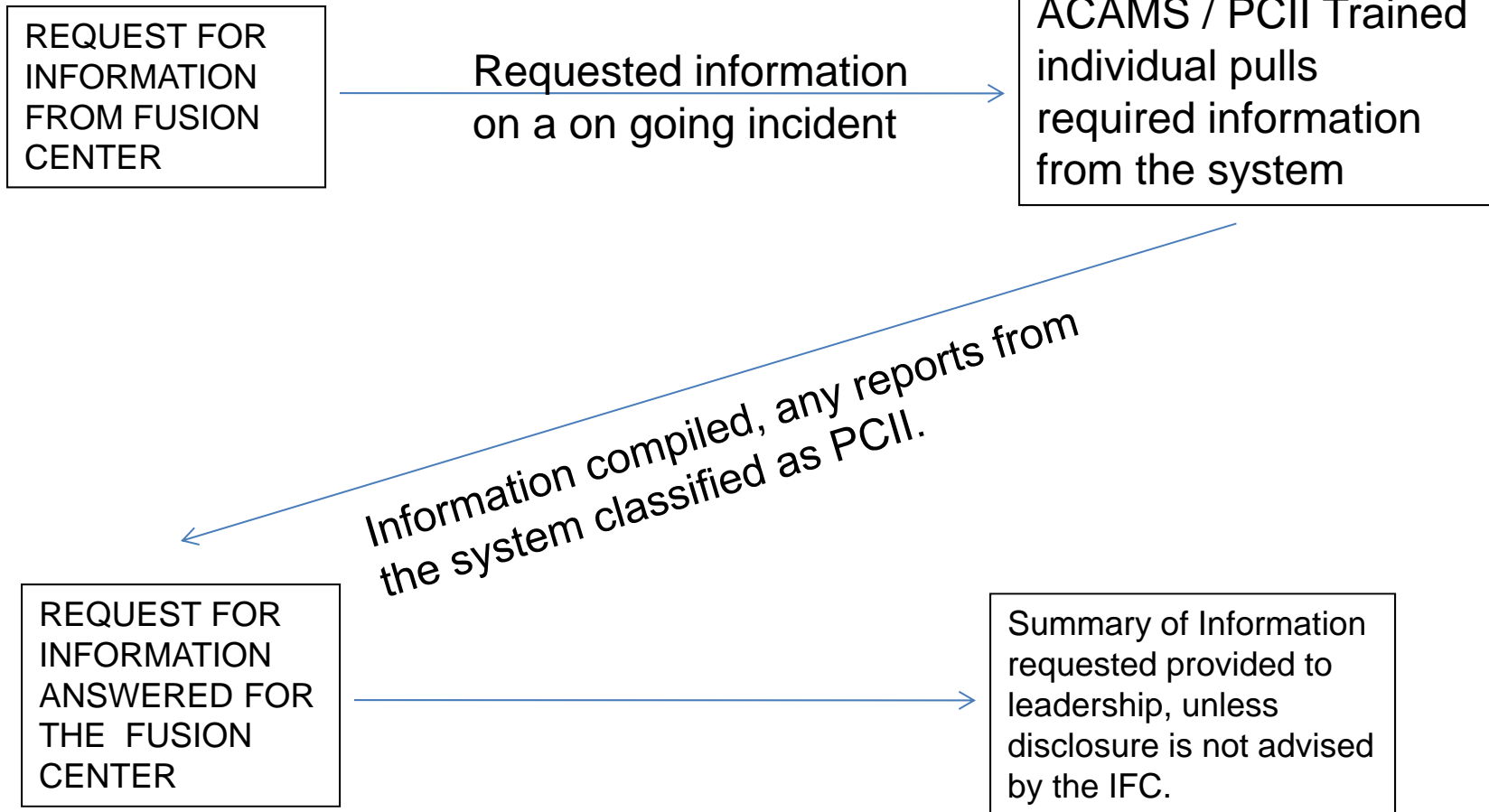
Communications Sector	
Control access to restricted areas to allow only authorized personnel.	
Limit parking around sensitive or restricted areas.	
Secure and regularly inspect all buildings, rooms, and storage areas on regular use.	
Consider 24-hour monitoring of security cameras.	
Include security and awareness trainings as part of daily job trainings.	
Train on communication lines, ensure communication plan is understood and practiced by all personnel.	
Minimize access vehicles leaving the facility.	
Implement roving security patrols in the buffer zone.	
Ensure the availability of sufficient technical resources to respond to and mitigate incidents.	
Verify that Continuity of Operations (COOP) site is in standby mode.	
Provide personnel with the following security possible threats, procedures for reporting suspicious activities, and the need for vigilance.	
Determine availability of emergency supplies.	
Train on employees exit to safe with customers concerning the facility or its operations.	
Suspend public tours of critical infrastructure facilities.	

FOR OFFICIAL USE ONLY

PAGE 1 of 1  
Email: tipp@iowa.gov

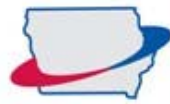
Advisory Released over HSIN to Sector Points of Contact for distribution

# TIIPP Overview (ACAMS)



# The Homeland Security Community

Law  
Enforcement



SAFEGUARD  
IOWA  
PARTNERSHIP

Public Safety

Surrounding  
States and  
Communities

Federal  
Agencies

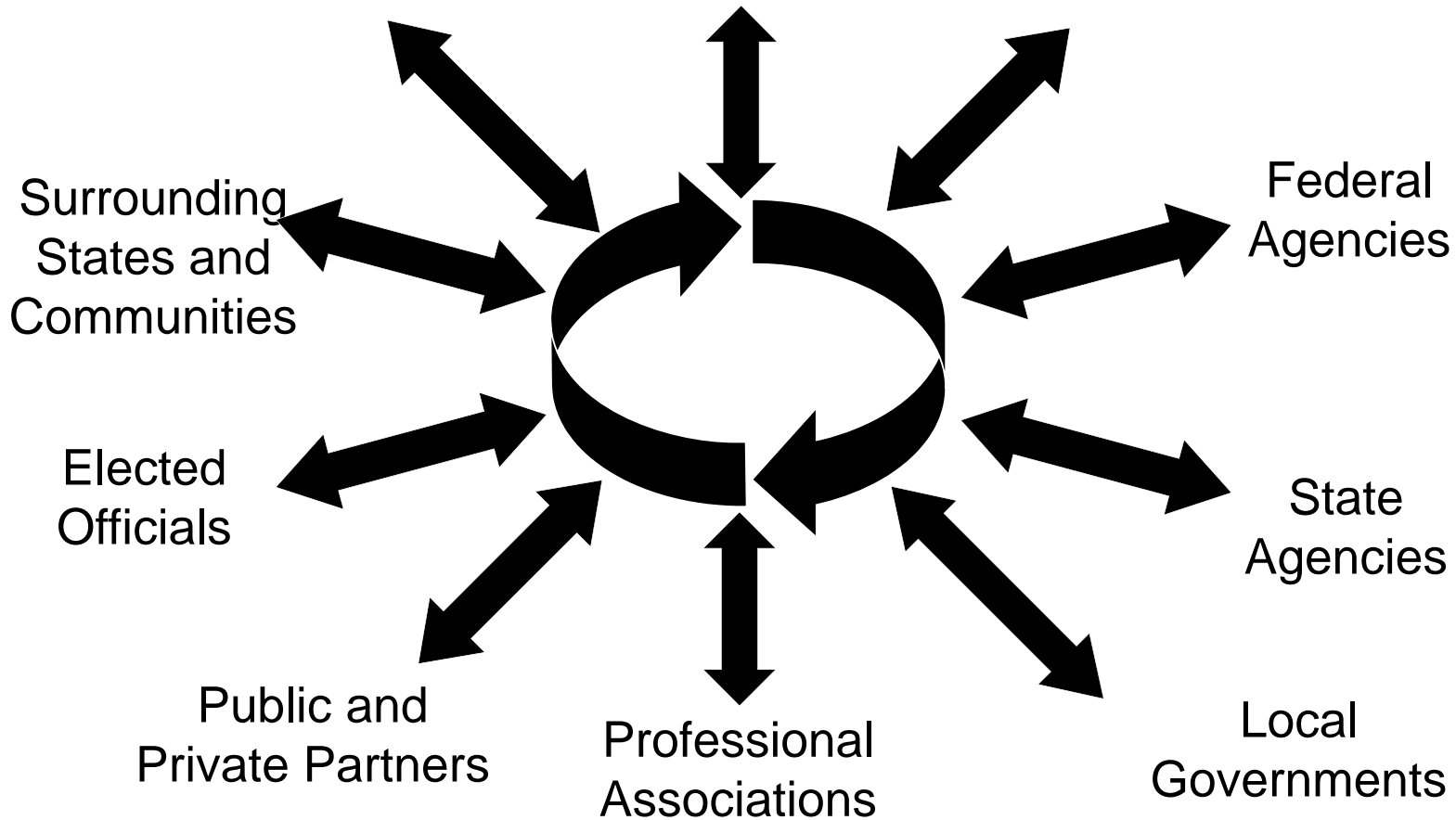
Elected  
Officials

State  
Agencies

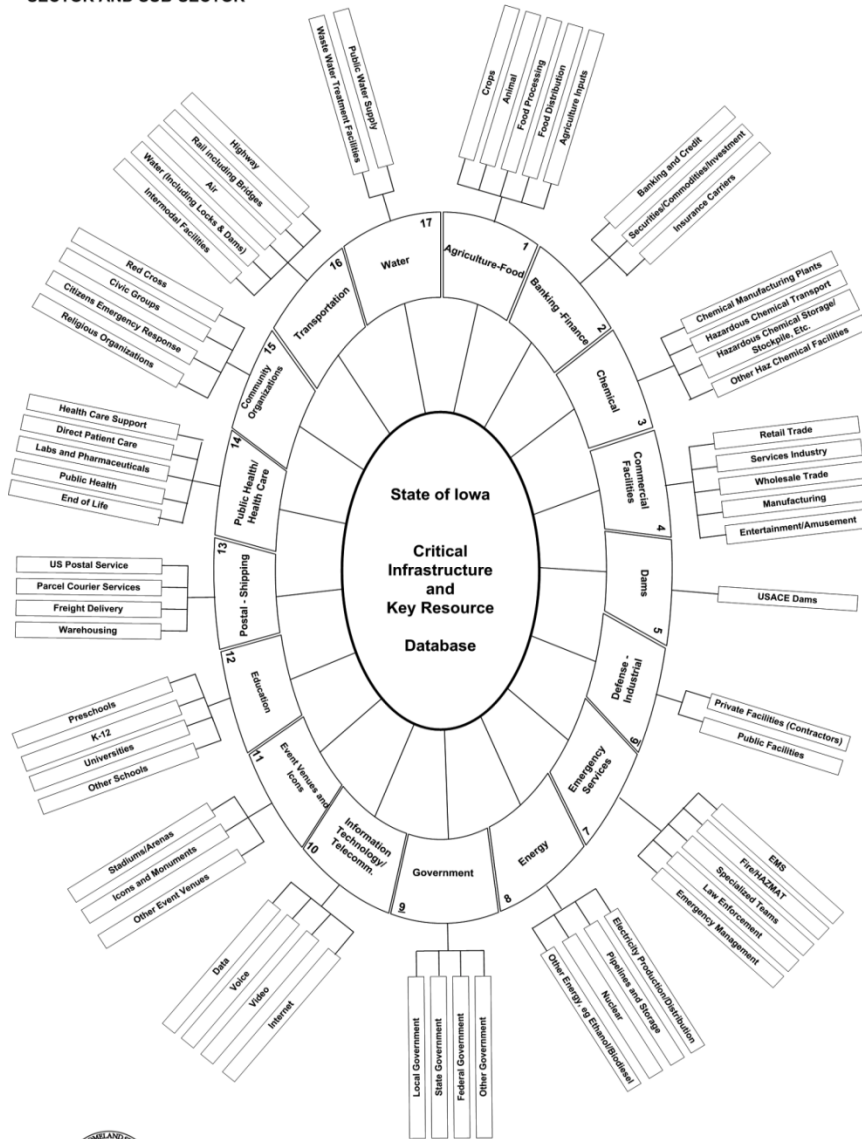
Public and  
Private Partners

Professional  
Associations

Local  
Governments



**STATE OF IOWA  
CRITICAL INFRASTRUCTURE / KEY RESOURCE DATABASE SCHEMATIC  
DRAFT  
SECTOR AND SUB-SECTOR**



December 2006

This document is subject to change as Sector and Sub Sector characteristics are refined.

## Critical Infrastructure Protection Plan (CIPP)

- Baseline Document on CIKR protection in Iowa.
- Proposed Name change to TIIPP Document.

## Sector Reference Documents

- Annexes to the CIPP
- Defining the sector in Iowa
- Asset categories
- Information sharing
- Interdependency study
- Updated with baselines gathered by the FSIVA assessments in the sector.

# The TIIPP DOES:

- Offers all hazards site assessments to address identified threats and vulnerabilities
- Process and distribute open-source information and sanitized law enforcement information
- Provides a voice for the critical infrastructure stake holders in the fusion process
- Creates mitigation recommendations through private sector advisories' when specific threats are identified
- Provide access to classified information and communications for approved state and local officials
- Assist in the coordination of state emergency response needs.
- Provide grant money to mitigate known weaknesses on identified critical infrastructure
- Offer training on Assessment Methodologies, ACAMS, and Risk Mitigation
- Responds to the DHS annual data call for critical assets, and events



**Iowa Homeland Security and Emergency Management Division**



# The TIIPP **DOES NOT**:

- exchange actionable criminal justice intelligence, unless specifically directed by the Iowa Department of Public Safety
- classify information for protection under federal or state law
- assume incident command and control or mission assign response assets



**Iowa Homeland Security and Emergency Management Division**

# Threat Information & Infrastructure Protection Program (TIIPP)

## Summary:

- Conducts site assessments as requested or threat specific
- On-going partnership between DPS and HSEMD
- Links intel with protection and preparedness
- Connects public and private protection activities
- Provides a link to homeland security information and operations



**Iowa Homeland Security and Emergency Management Division**



# Questions?

- Curt Sullivan: 725-3202/250-9336
- [Curt.sullivan@iowa.gov](mailto:Curt.sullivan@iowa.gov)
- Brian Lewis: 725-3209/515-979-2793
- [Brian.lewis@iowa.gov](mailto:Brian.lewis@iowa.gov)