Georgia's Cyber Defense
A Management Brief

April 2013

GISAC Cyber Responsibility

"Each Chief Executive of a State, local, tribal or territorial government is responsible for its cyber security preparedness, response and recovery procedures as outlined in the Roles and Responsibilities "

…National Cyber Incident Response Plan 2010 – US Dept. of Homeland Security

Georgia's Fusion Center

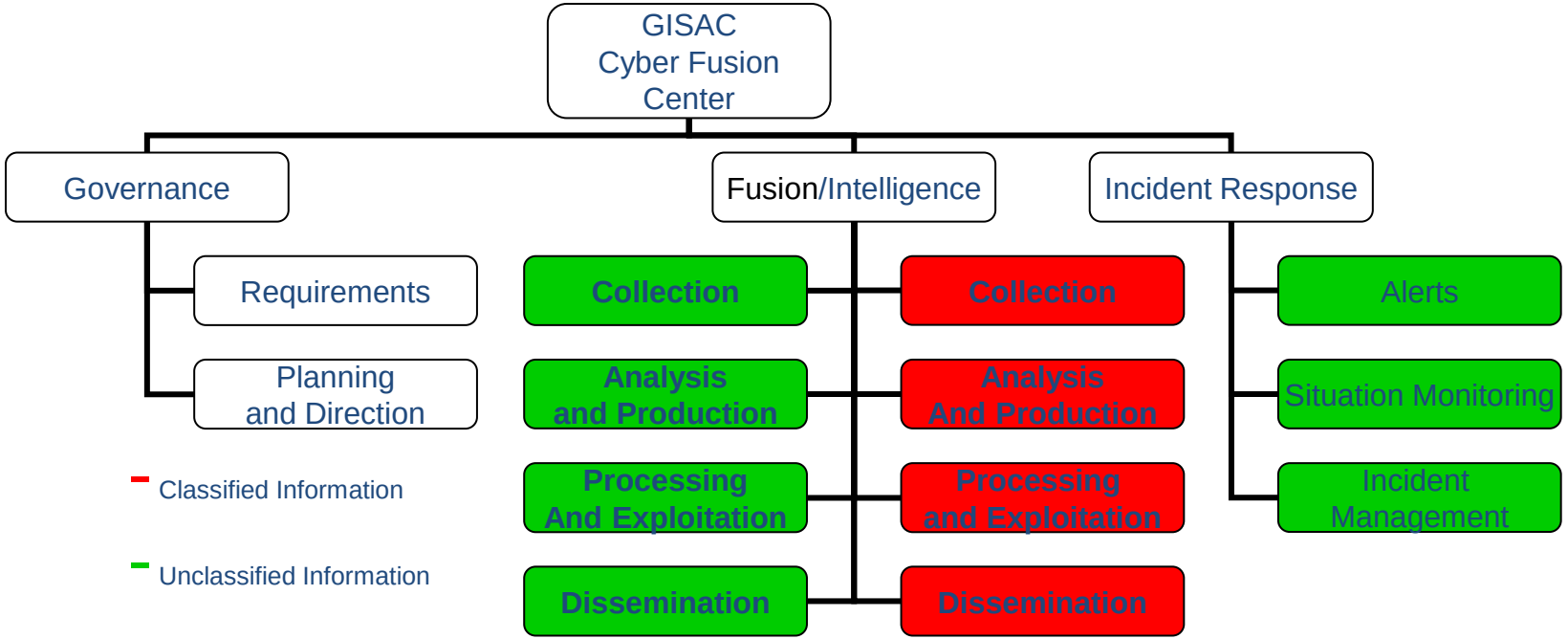
"Fusion: Turning Information and Intelligence Into Actionable Knowledge"

…Fusion Center Guidelines, US Dept. of Justice

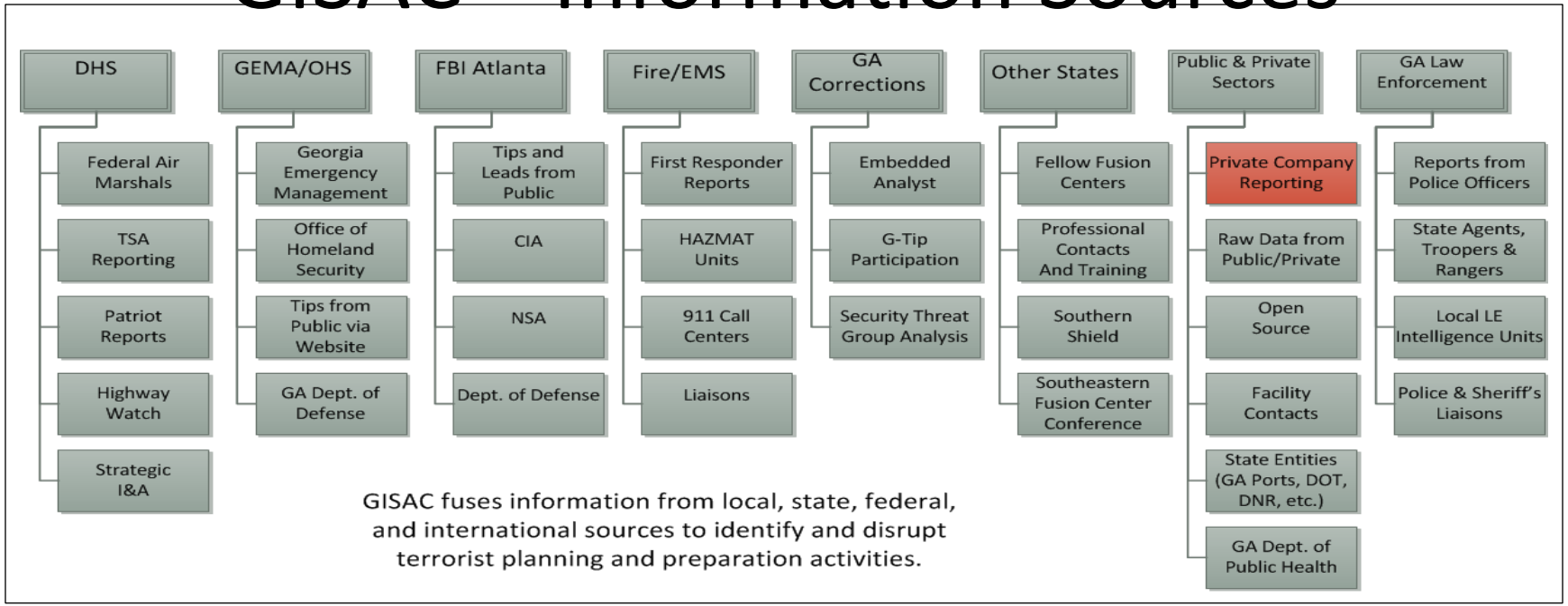
GISAC Cyber Objectives

- **Situation Awareness:** Alerts, Bulletins, and Reports
- **Cyber Incident Response:** Planning, Exercises, Incident Management
- **Cyber Threat and Vulnerability:** Assessments
- **Research:** Cyber terrorism-crime, Hacktivism
- **Outreach and Information Sharing**: Education, Private Sector, and Expansion

Functional Areas and Processes



GISAC – Information Sources



Unspoken Risks: State IT Infrastructure

Critical Infrastructure Key Resources

Critical Infrastructure

- Chemical
- Commercial Facilities
- Communications
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Facilities
- Healthcare and Public Health
- Information Technology
- National Monuments and Icons
- Nuclear Reactors, Materials and Waste
- Postal and Shipping
- Transportation
- Water and Wastewater Systems

Is Situation Awareness A Compliance Activity?

Yes!

(you're not done)

Compliance Artifacts

- Each agency should have an inventory of all systems.
- For each system, there should be:
  - A system security plan.
  - An assessment report including risks.
  - A formal authorization to operate accepting risks.
- A combined prioritized risk registry for the agency.
- A process for managing residual risks and identifying new risks.

Georgia Must Become More Aware

- Compliance with FISMA requires on ongoing risk management process, including situational monitoring.
- The Fusion Center identifies new threats and vulnerabilities.
- Agencies must integrate Fusion Center products into their ongoing monitoring process.
- Agencies must continue to improve their security.

Georgia