eGuardian

eGuardian Brief

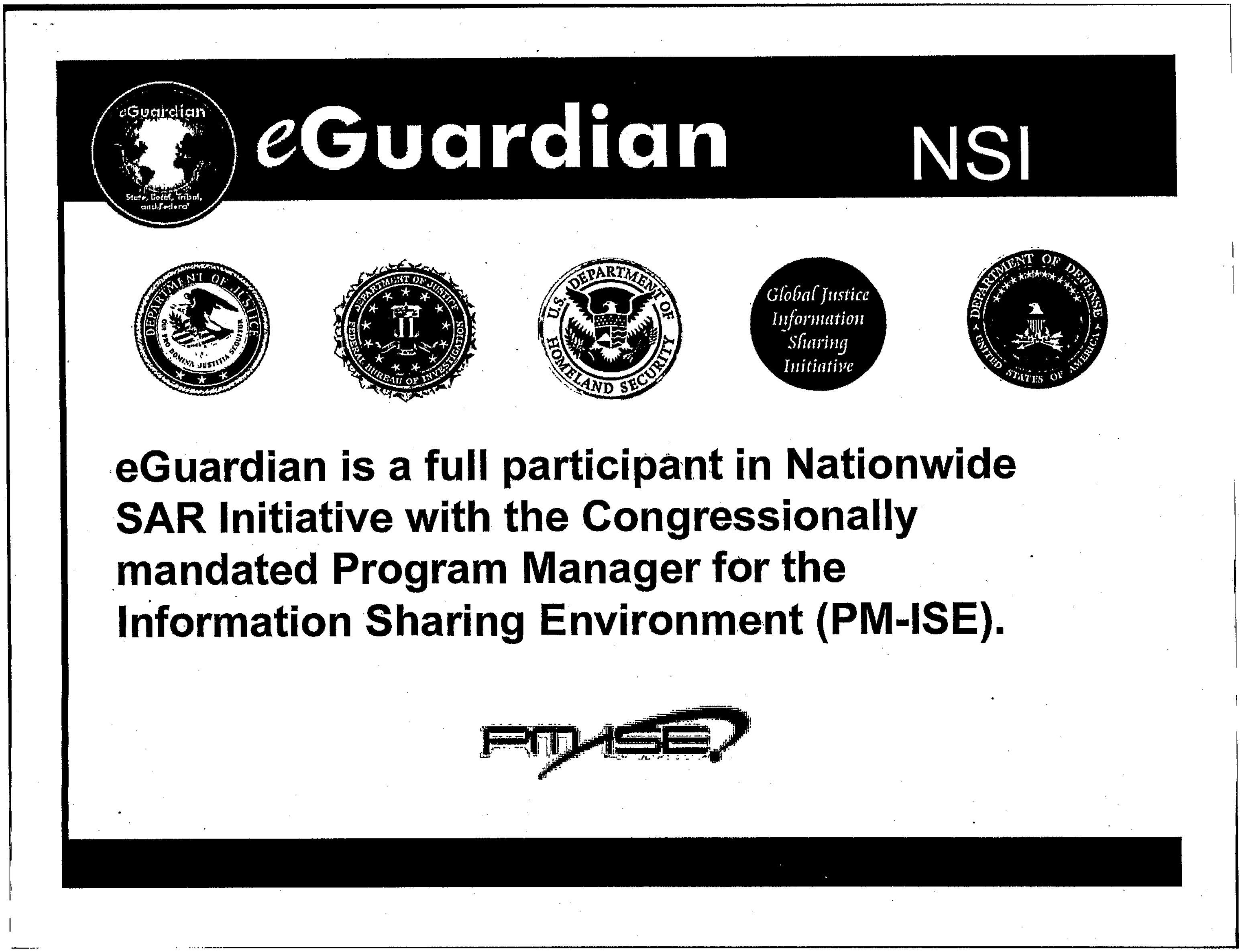
IACP 2009

Sharing as it evolves from the "need to know" to the "need to share"— to now "the responsibility to provide"

—Ambassador [redacted]
[redacted] *Information Sharing Environment (PM-ISE)*

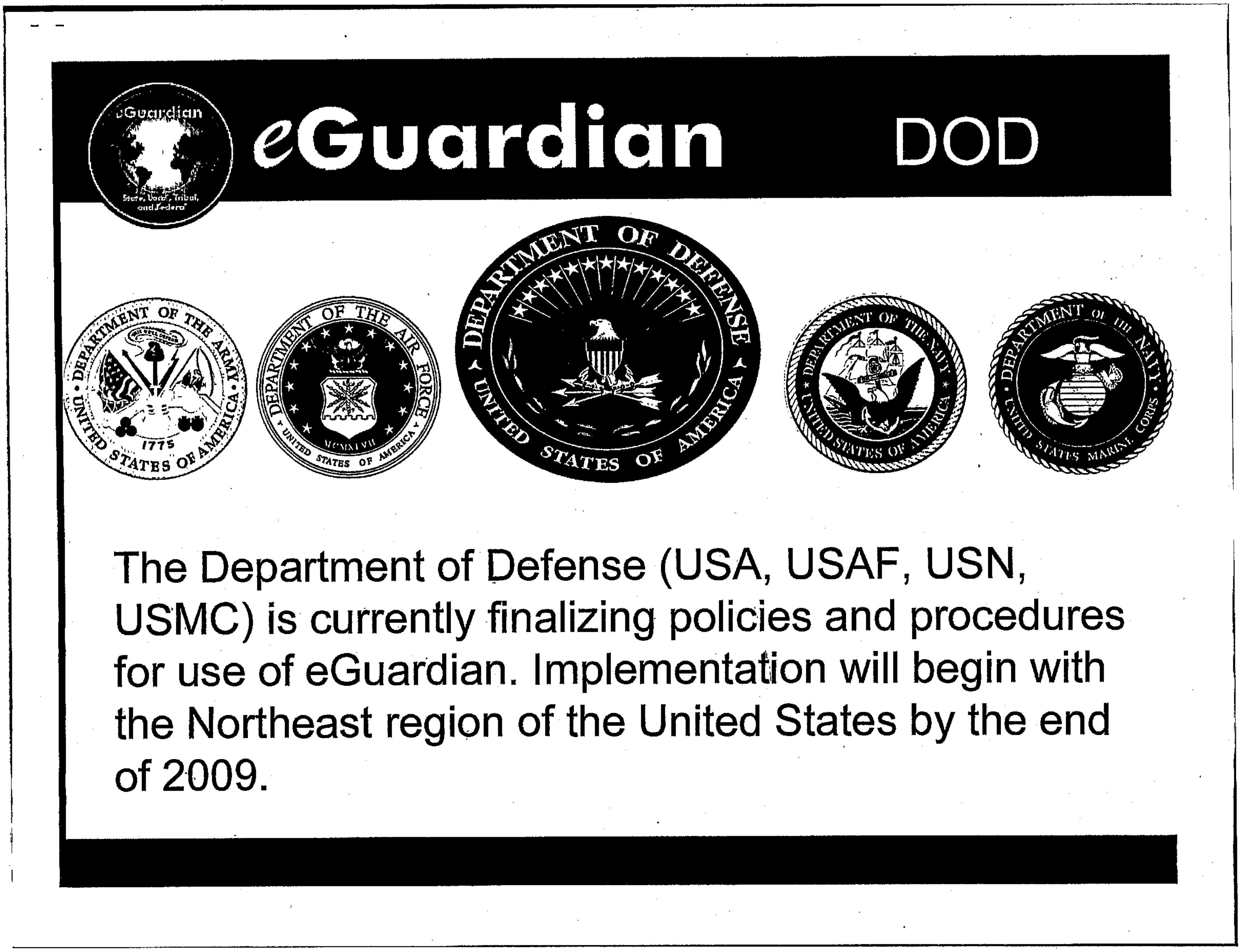
b6
b7C

The overall classification of this brief is: UNCLASSIFIED/Law Enforcement Sensitive



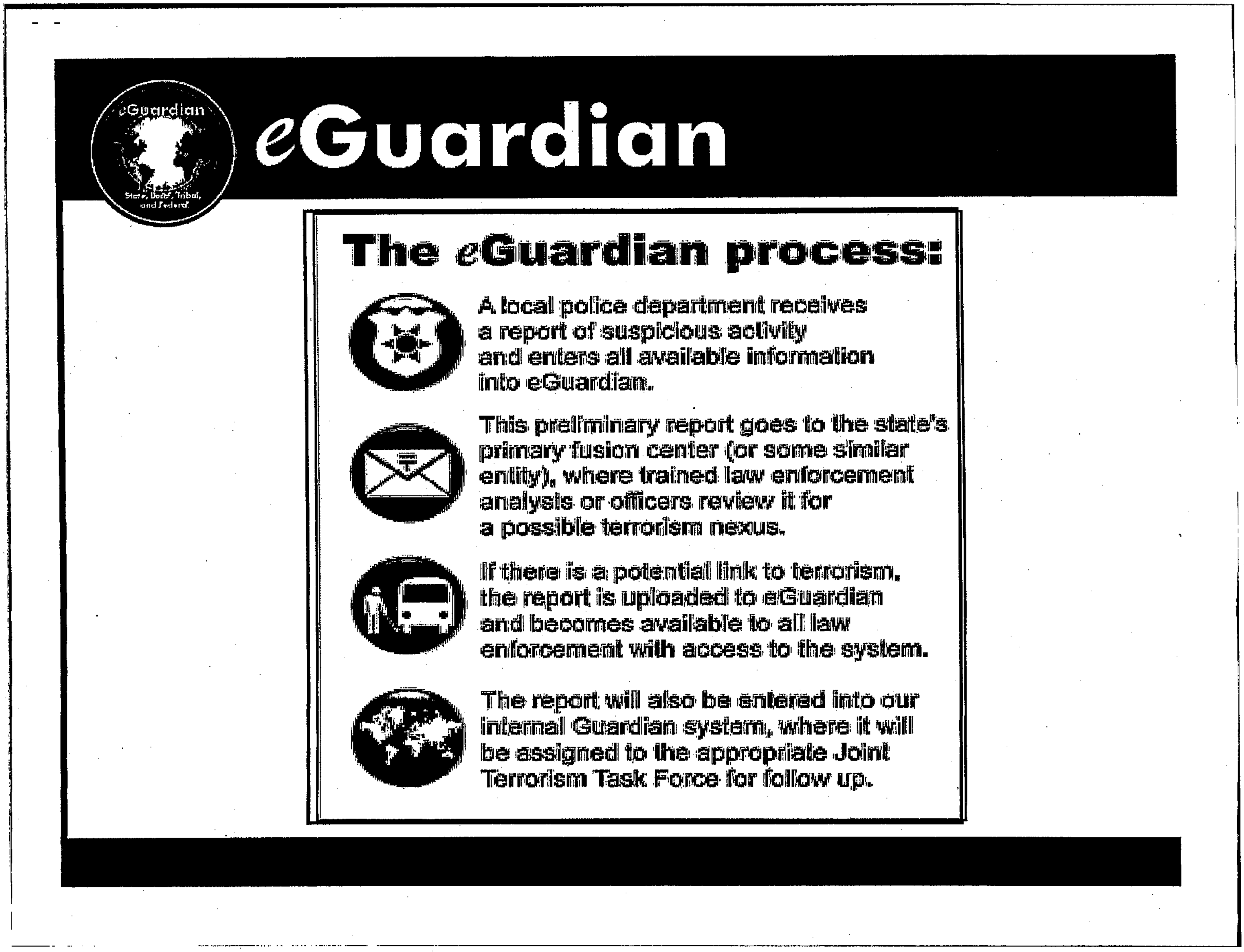
eGuardian NSI

eGuardian is a full participant in Nationwide SAR Initiative with the Congressionally mandated Program Manager for the Information Sharing Environment (PM-ISE).



eGuardian DOD

The Department of Defense (USA, USAF, USN, USMC) is currently finalizing policies and procedures for use of eGuardian. Implementation will begin with the Northeast region of the United States by the end of 2009.



eGuardian

The eGuardian process:

A local police department receives a report of suspicious activity and enters all available information into eGuardian.

This preliminary report goes to the state's primary fusion center (or some similar entity), where trained law enforcement analysts or officers review it for a possible terrorism nexus.

If there is a potential link to terrorism, the report is uploaded to eGuardian and becomes available to all law enforcement with access to the system.

The report will also be entered into our internal Guardian system, where it will be assigned to the appropriate Joint Terrorism Task Force for follow up.

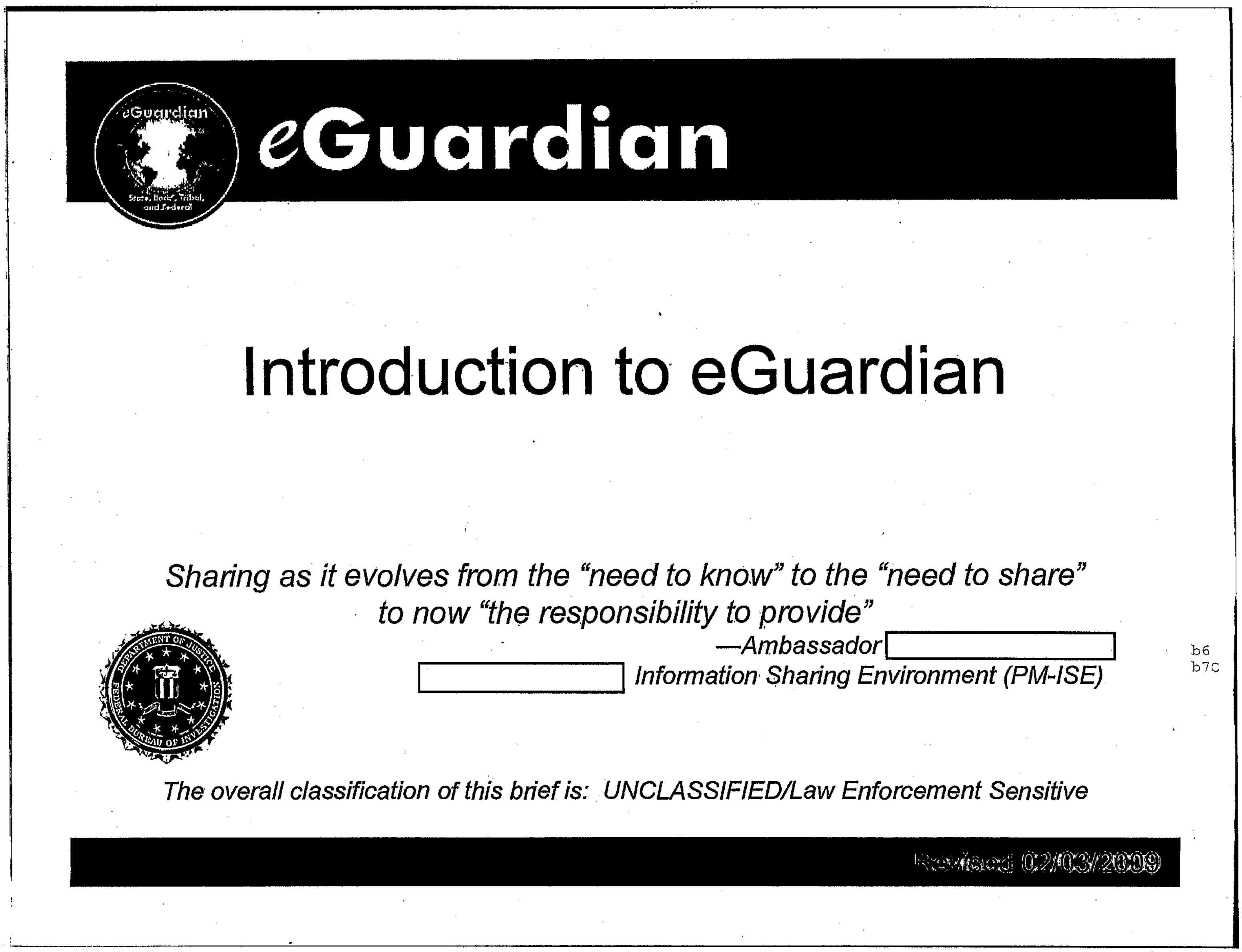
*e*Guardian

Questions?

For Access Go To: www.leo.gov

LEO Help Desk: 1-888-334-4536

eGuardian Help Desk: 1-866-672-9763



eGuardian

Introduction to eGuardian

Sharing as it evolves from the "need to know" to the "need to share" to now "the responsibility to provide"

—Ambassador [redacted]

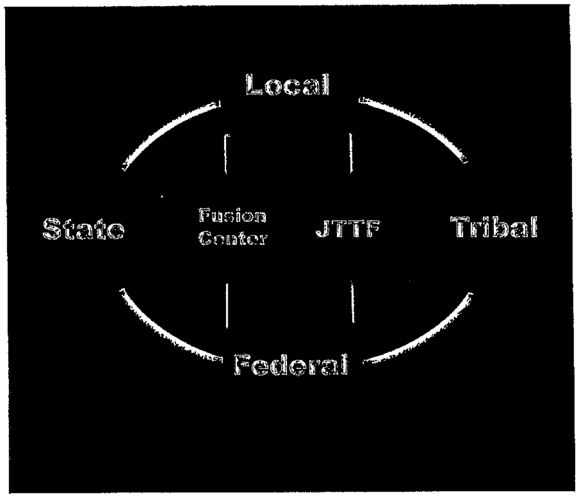
[redacted] Information Sharing Environment (PM-ISE)

b6
b7C

The overall classification of this brief is: UNCLASSIFIED/Law Enforcement Sensitive

Revised 02/03/2009

eGuardian



Local

State

Fusion Center

JTTF

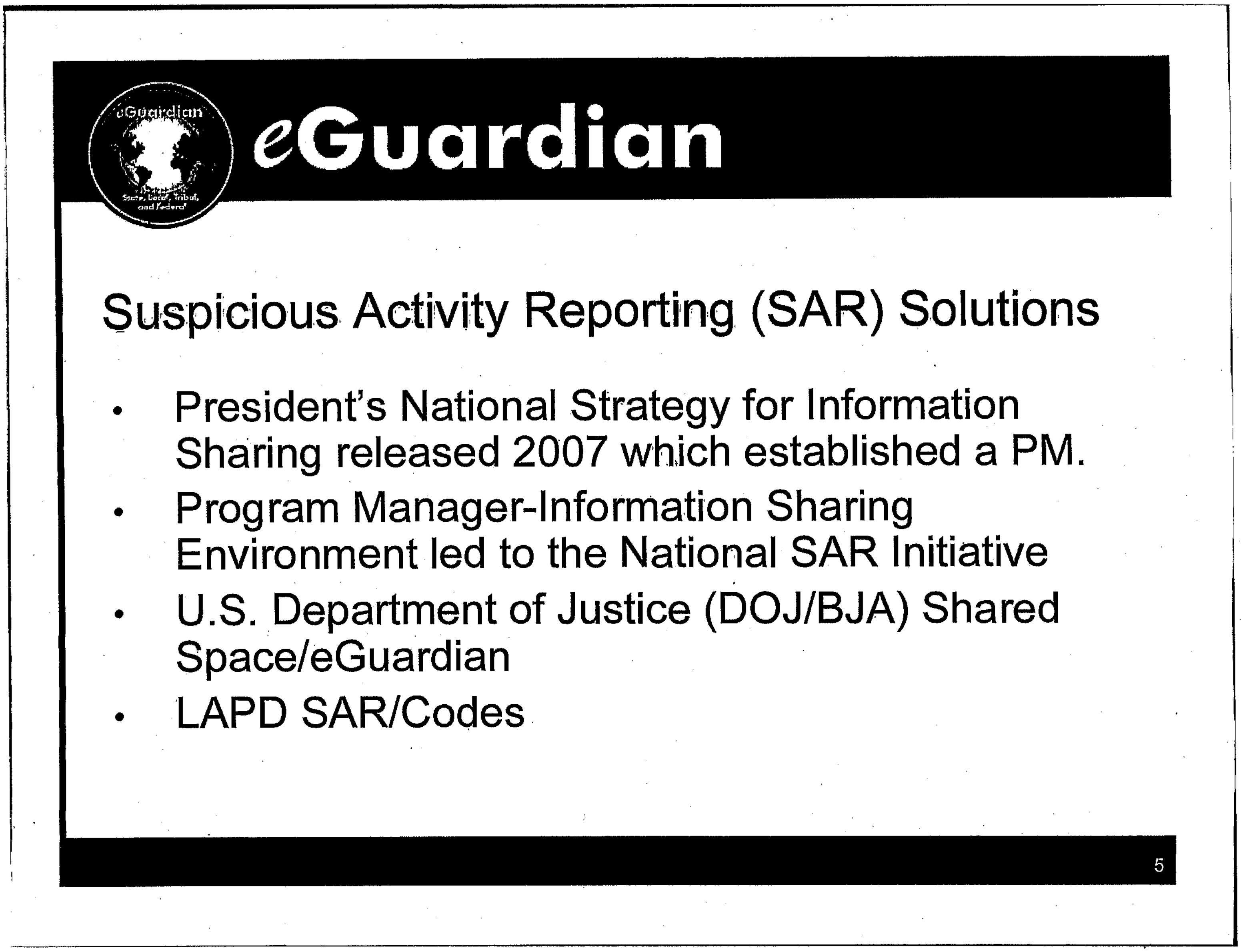
Tribal

Federal

eGuardian is a secure, user-friendly system implemented to share potential terrorist threats, terrorist events, and suspicious activity among the state, local, tribal, and federal law enforcement partners along with state fusion centers and the Federal Bureau of Investigation Joint Terrorism Task Forces (JTTFs)

eGuardian

- SARs are collected everyday
- Information gathered may be a precursor to criminal activity to include terrorism
- Sharing information can prevent or solve crimes and even save lives when linked together
- Although technology plays a key role linking information there still needs to be human interaction verifying the information to ensure the protection of an individual's privacy and civil liberties



eGuardian

Suspicious Activity Reporting (SAR) Solutions

- President's National Strategy for Information Sharing released 2007 which established a PM.
- Program Manager-Information Sharing Environment led to the National SAR Initiative
- U.S. Department of Justice (DOJ/BJA) Shared Space/eGuardian
- LAPD SAR/Codes

eGuardian

Reporting Versus Recording System

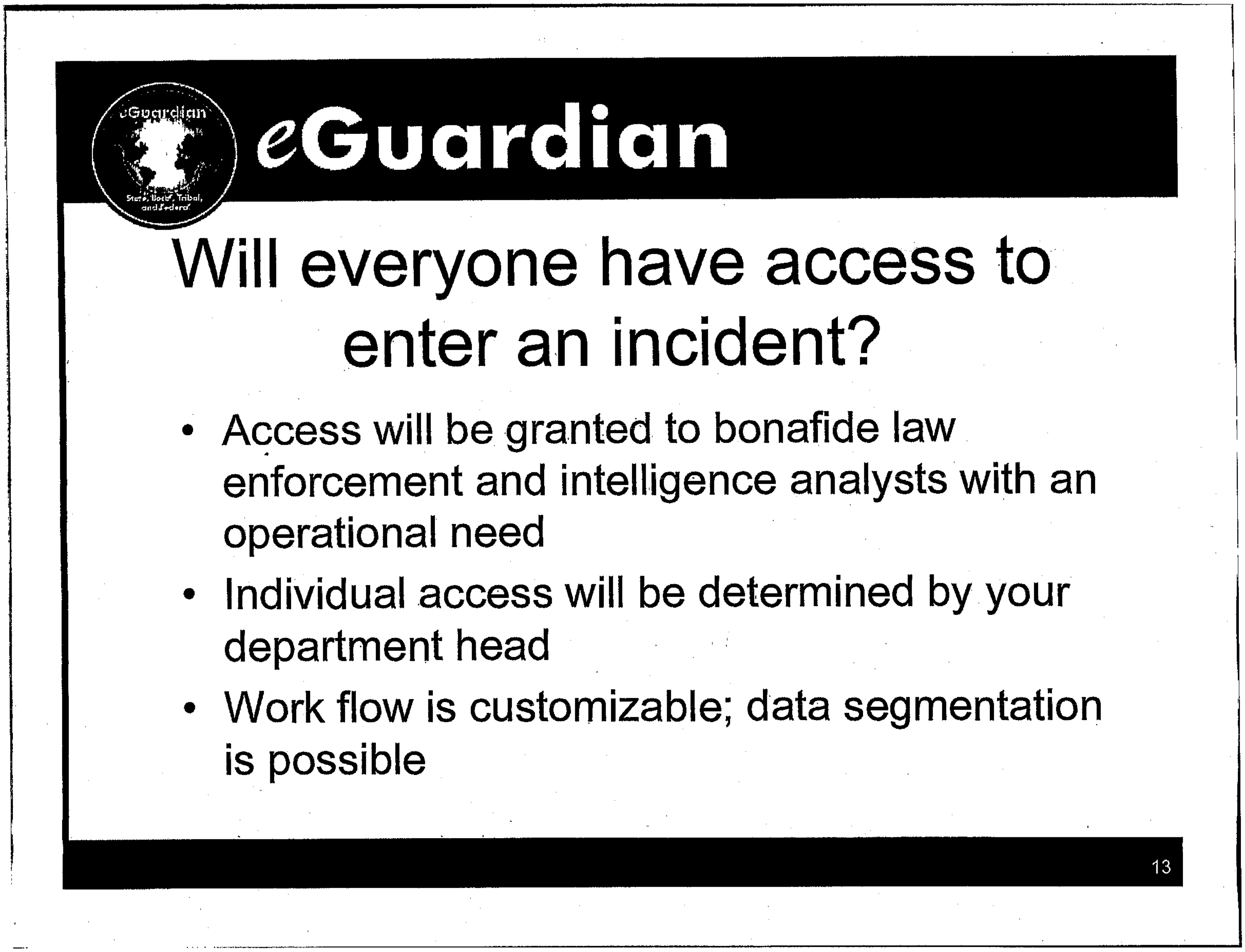
- eGuardian is a non-emergency threat management system designed to share suspicious activity and threats with a potential nexus to terrorism
- eGuardian is designed to record threats and share them among its partners
- eGuardian ensures increase in the number of quality incidents provided to the FBI JTTF for investigation

eGuardian

Law Enforcement Online

- LEO is a 24-hour-a-day, 7-day-a-week online (real-time), controlled-access communications and information sharing data repository
- Provides Internet-accessible focal point for electronic Sensitive But Unclassified (SBU) communication and information sharing
- Users anywhere in the world can communicate securely using LEO
- [redacted]

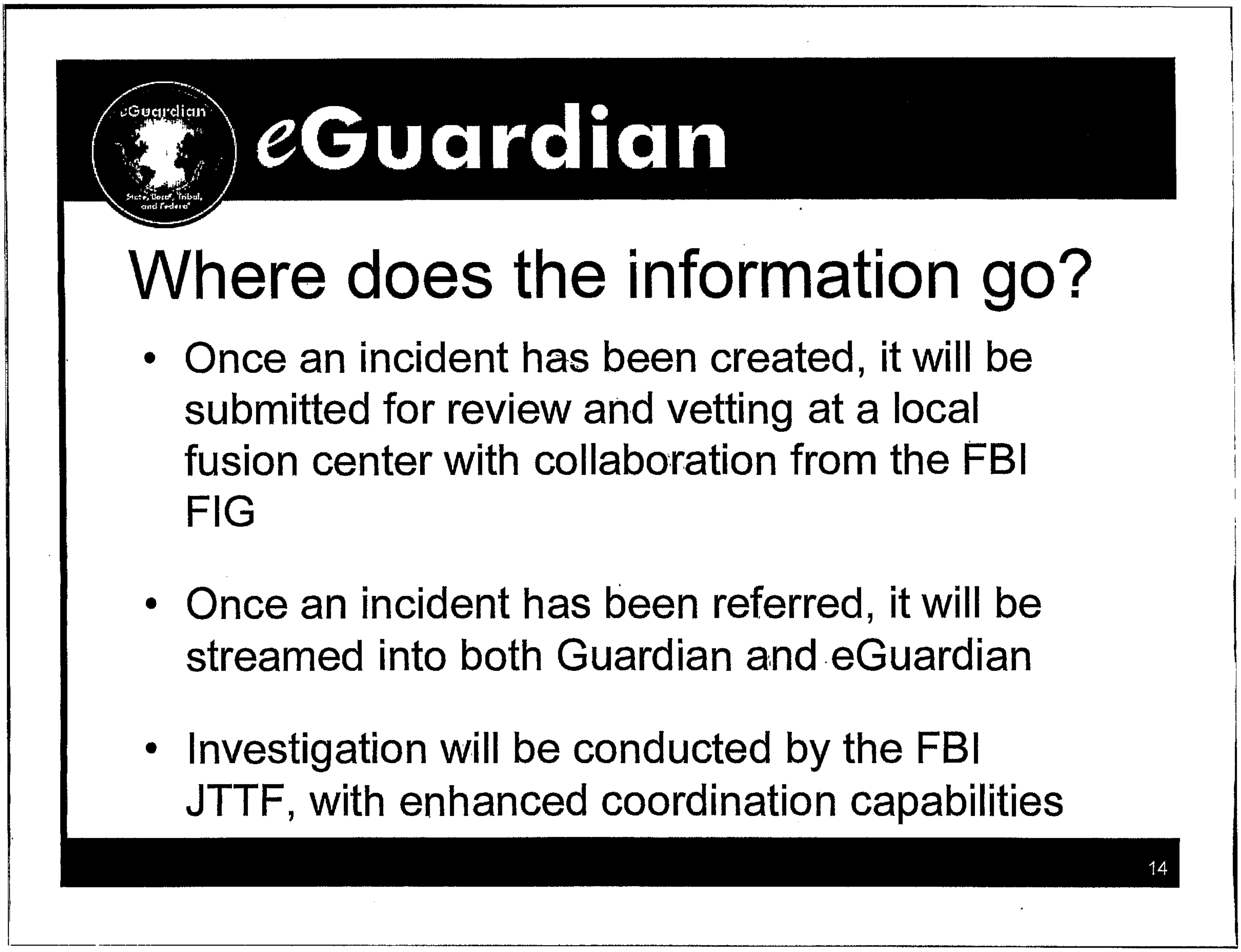
b7E



eGuardian

Will everyone have access to enter an incident?

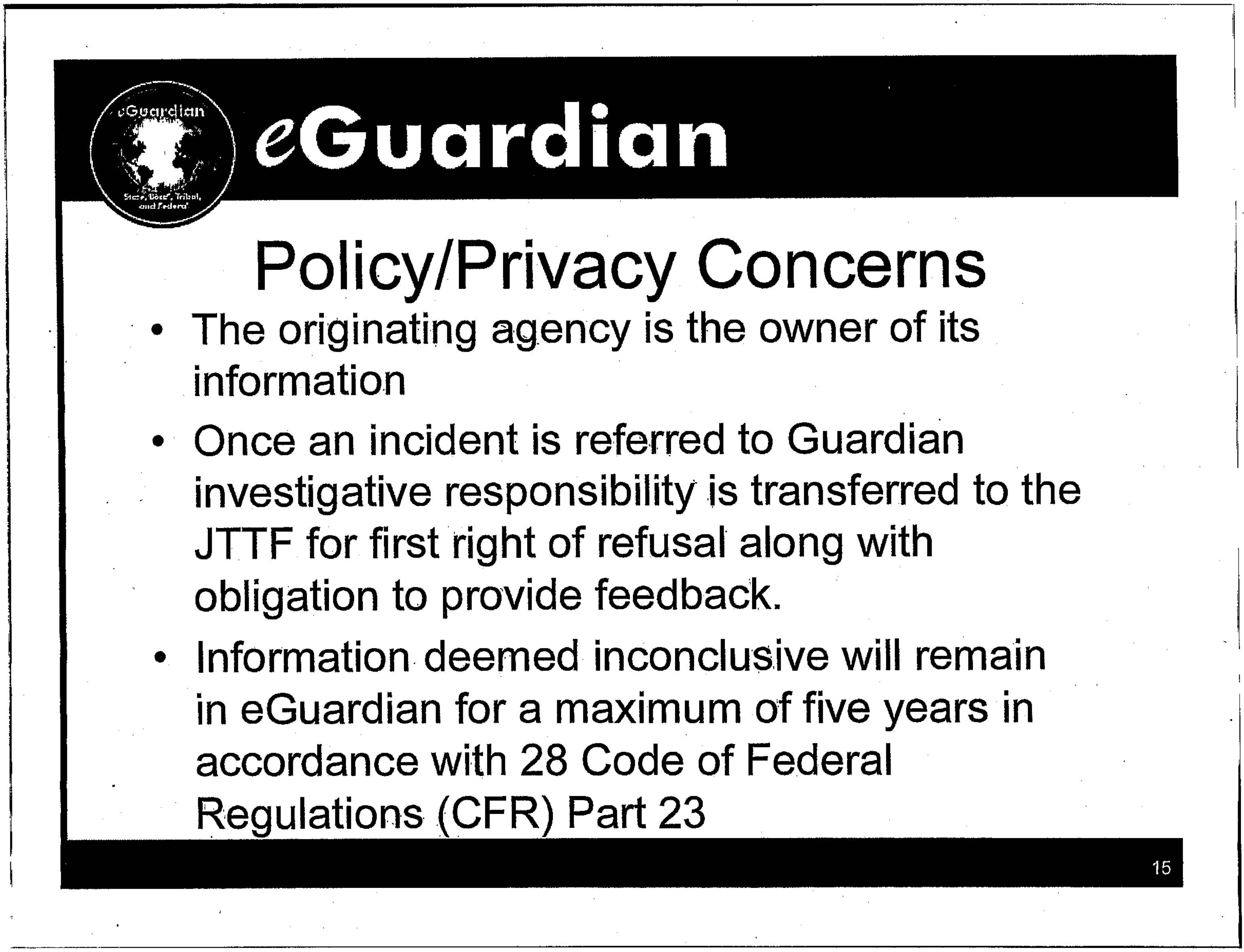
- Access will be granted to bonafide law enforcement and intelligence analysts with an operational need
- Individual access will be determined by your department head
- Work flow is customizable; data segmentation is possible



eGuardian

Where does the information go?

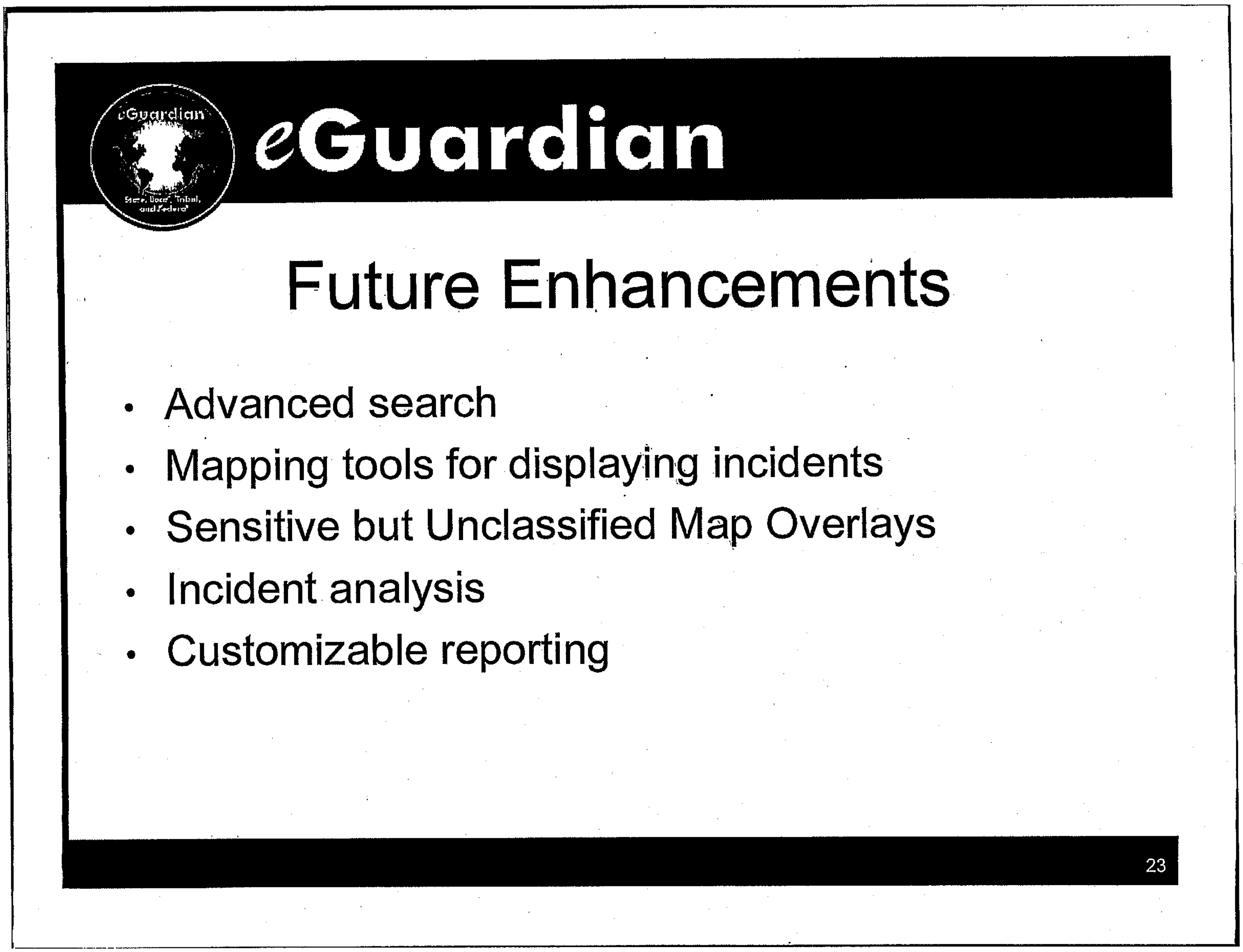
- Once an incident has been created, it will be submitted for review and vetting at a local fusion center with collaboration from the FBI FIG
- Once an incident has been referred, it will be streamed into both Guardian and eGuardian
- Investigation will be conducted by the FBI JTTF, with enhanced coordination capabilities



eGuardian

Policy/Privacy Concerns

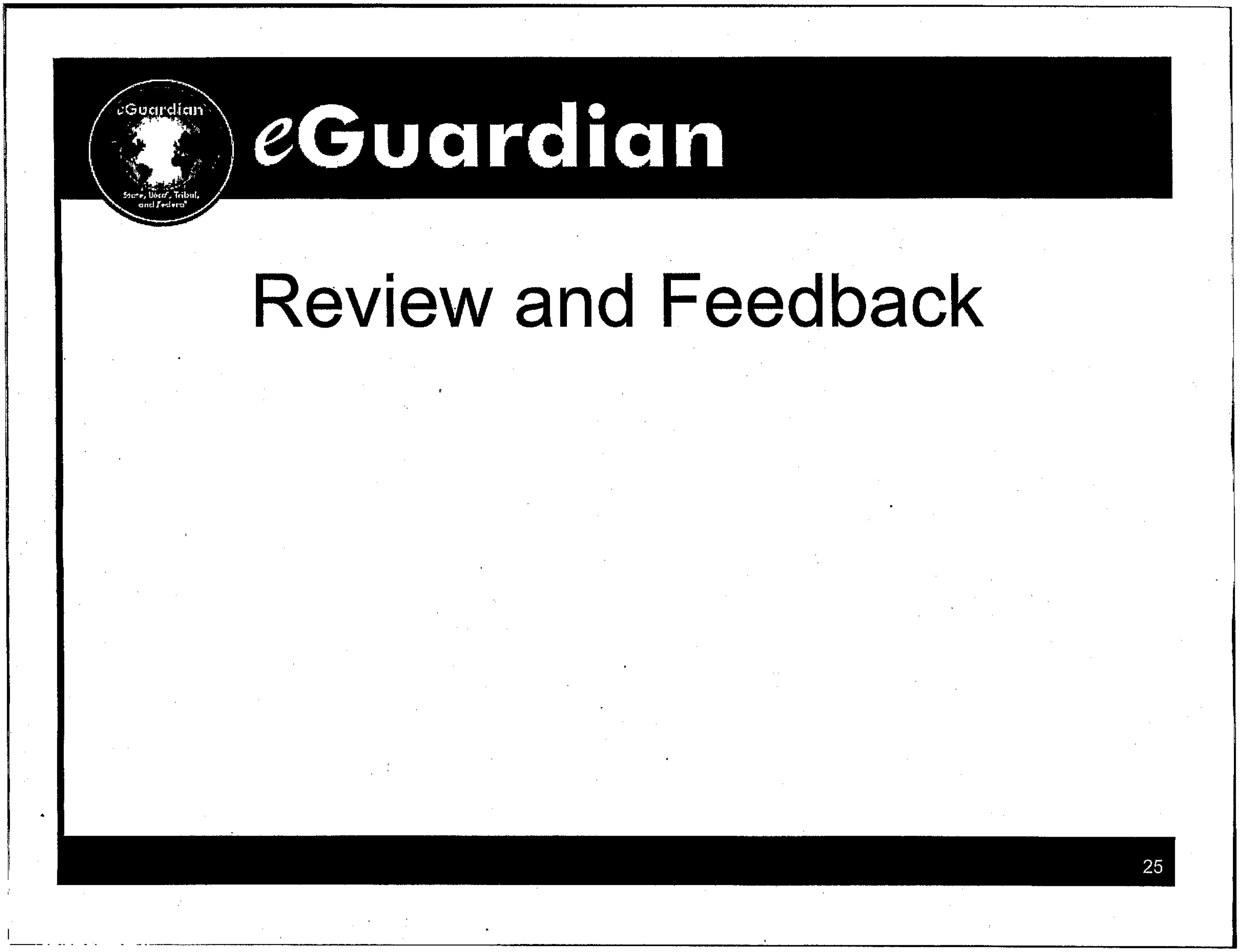
- The originating agency is the owner of its information
- Once an incident is referred to Guardian investigative responsibility is transferred to the JTTF for first right of refusal along with obligation to provide feedback.
- Information deemed inconclusive will remain in eGuardian for a maximum of five years in accordance with 28 Code of Federal Regulations (CFR) Part 23



*e*Guardian

Future Enhancements

- Advanced search
- Mapping tools for displaying incidents
- Sensitive but Unclassified Map Overlays
- Incident analysis
- Customizable reporting



Review and Feedback