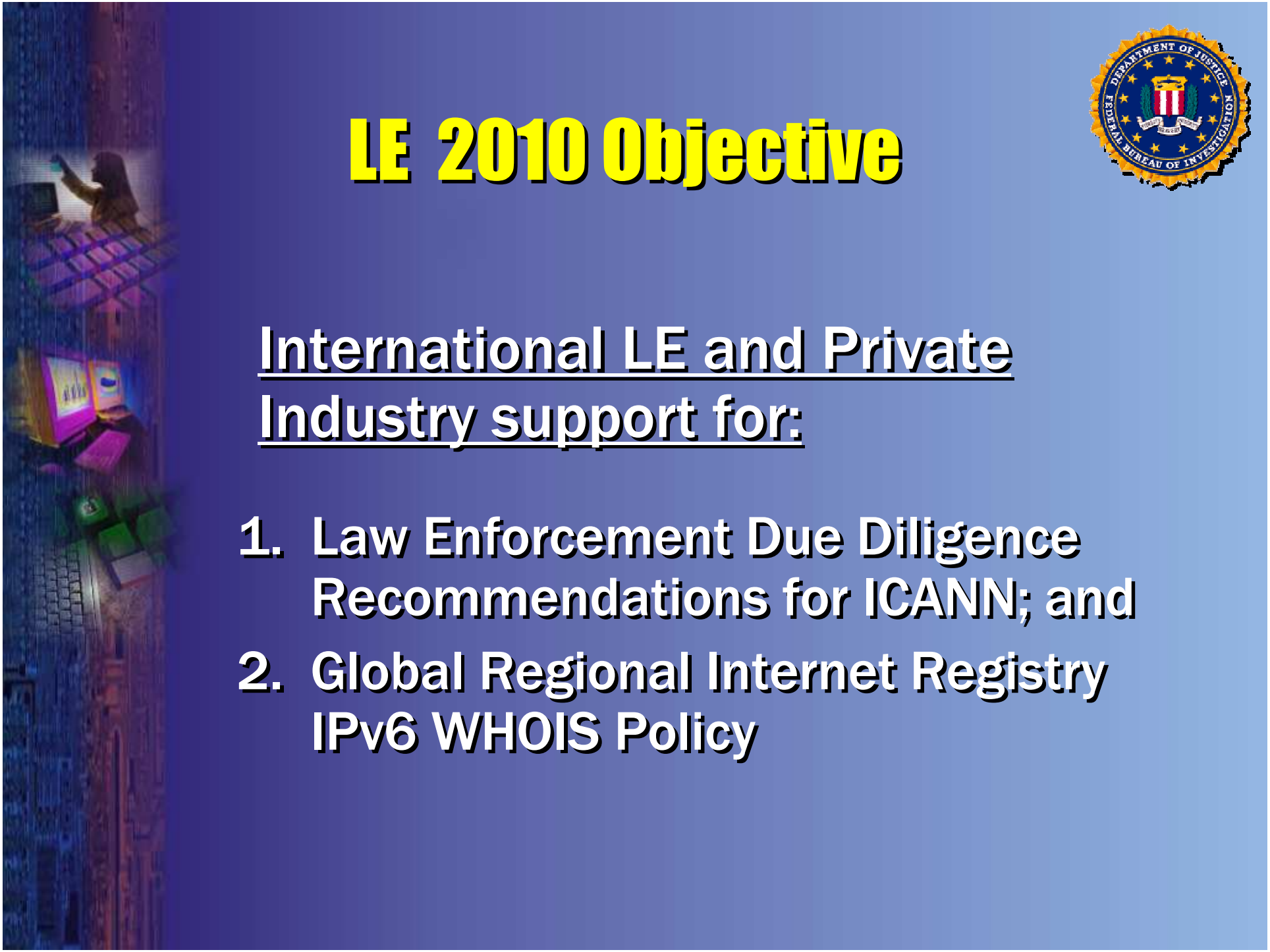
Law Enforcement - Internet Governance Initiatives - 2010

Supervisory Special Agent Robert Flaim
Federal Bureau of Investigation (FBI)
Paul Hoare – Senior manager
Serious Organised Crime Agency (SOCA)

Goal of this Presentation

- Explanation of DNS and IP/ASN Internet Governance organizations
- LE Proposals before these organizations
- How LE can support these proposals and move toward passage and enactment



LE 2010 Objective

International LE and Private Industry support for:

1. Law Enforcement Due Diligence Recommendations for ICANN; and
2. Global Regional Internet Registry IPv6 WHOIS Policy

LE and Internet Governance Organizations

- Internet Corporation of Assigned Names and Numbers (ICANN)
- Regional Internet Registries (RIR)
  - AfriNIC
  - ARIN
  - APNIC
  - LACNIC
  - RIPE NCC

What is ICANN ?

- Founded in 1998 as a not-for-profit organization
- Coordinates the allocation and assignment of the three sets of unique identifiers for the Internet, which are:
  - Domain names (forming a system referred to as "DNS");
  - Internet protocol ("IP") addresses and autonomous system ("AS") numbers; and
  - Protocol port and parameter numbers
- Coordinates the operation and evolution of the DNS root name server system.

Top Level Technical Coordination Body

Current LE Due Diligence and RAA Proposal for ICANN

Recommendations to ICANN

LE presented Due Diligence and RAA Improvement Proposal to ICANN Board, the GAC and ICANN Community at ICANN Seoul Meeting, October 2009

Supported by:

- G-8 High Tech Crime Group,
- Interpol Cyber Working Group

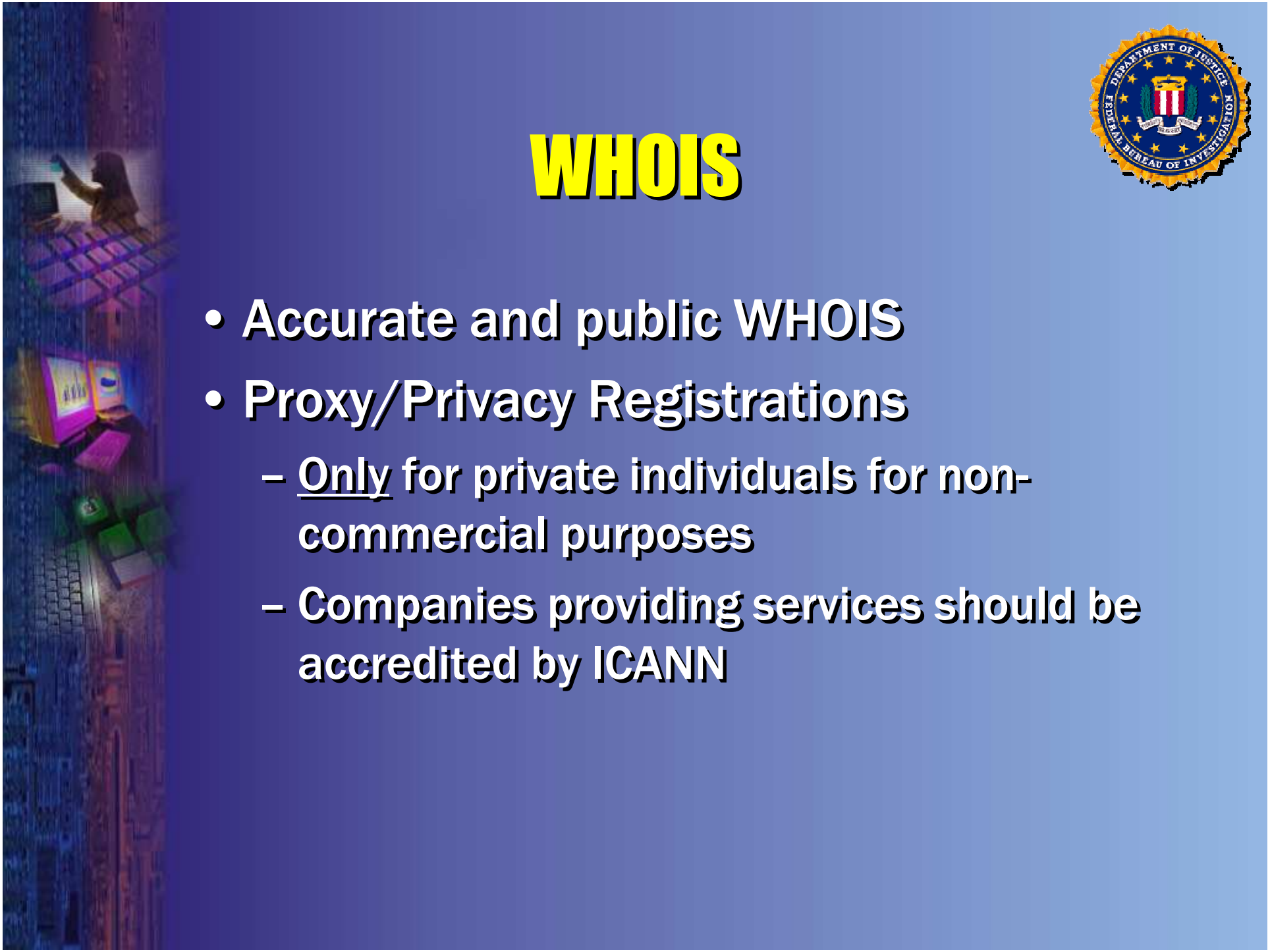
LE Due Diligence Proposal

Three (3) Objectives of LE Proposal:

1. Due Diligence
2. WHOIS
3. Transparency and Accountability

Due Diligence

- ICANN needs to vet potential registrars and registries, through checks of international databases to ascertain an organization's good standing, i.e.,
  - Dun and Bradstreet
  - Lexus Nexus
- Registrars need to validate data received at time of domain name registration and periodically thereafter, i.e.,
    - Time-based algorithms, IP, BIN data, HTTP header information and device ID, blacklists, null values, etc.



WHOIS

- Accurate and public WHOIS
- Proxy/Privacy Registrations
  - Only for private individuals for non-commercial purposes
  - Companies providing services should be accredited by ICANN

Accountability and Transparency

- Domain name resellers and all third party beneficiaries to be held to the same terms and conditions as Registrars
- ICANN should require all registrars, registries, proxy services, resellers and all third party beneficiaries of any contracts, policies of ICANN to publicly display ownership, parent companies, subsidiaries and business associations

Regional Internet Registries (RIR)

- RIRs allocate IP addresses and Autonomous System Numbers (ASN).
- RIRs receive their IP/AS Numbers from IANA (Internet Assigned Numbers Authority)…which is administered by ICANN.

Regional Internet Registries (RIR)

Why LE/Government- RIR Working Groups?

To go from reactive to proactive;

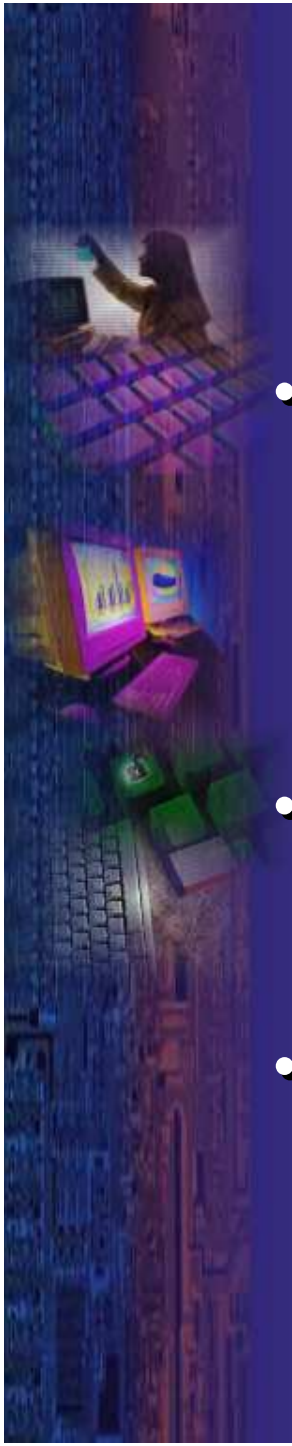
- LE coordinate with RIRs and private industry to develop policies that will enhance LE capabilities in crime-fighting for the safety and security of the Internet
- Issues addressed in RIPE NCC, ARIN:
  - IP revocation
  - WHOIS policies
  - IPv4 Network Address Translation
  - IPv6 WHOIS, allocation policies

LE-RIR Working Groups

Creation of LE/Government Working Groups

- RIPE NCC started RIPE NCC Cooperation (Government) WG in 2005
  - LE first attended in September 2008
- ARIN established ARIN Government WG (AGWG) in February 2009
- AfriNIC created AfGWG with LE January 2010
- LACNIC discussed WG May 2009
  - LE from Brazil, Uruguay, Costa Rica and Nicaragua
- APNIC and Australian Federal Police negotiations for LE/Government WG

LE Issues Addressed at RIRs



- WHOIS - Working with ARIN for open and accurate WHOIS, have persuaded ARIN to not limit WHOIS, despite several policy proposals and have successfully defeated such policies;

- IP Revocation – RIPE NCC: Exercise of due diligence in allocating IP addresses

- Common-carrier Network Address Translation (NAT) - Coordinating with ARIN and authors of IETF proposal, i.e. ensuring proper logging.

Outstanding Issues - RIRs and ICANN

- Strengthen existing IPV4 WHOIS policies
- Introduce IPv6 Global RIR policy
  - Ensure all organizations holding IPv6 allocations or assignments maintain complete, accurate and current customer information for both organizations and points of contact, i.e., WHOIS
  - Draft of policy introduced at E-Crime Congress in London, March 17th

Action Plan - ICANN

- Support LE ICANN Due Diligence Proposal – How?
  - Attend ICANN Brussels Meeting on June 21, 2010
  - Tell your ICANN GAC representative to support GAC endorsement of LE Due Diligence Proposal
  - http://gac.icann.org/gac-representatives
- Gather statistics or "war stories" to present at ICANN Brussels:
  - False domain name WHOIS data
  - Proxy registrations
  - Criminal Registrars
  - Difficulty in locating registrar to serve legal process
  - Registrar havens for "criminal" domain

ICANN Brussels
June 20-23, 2010

- GAC – LE meet with GAC to gain GAC endorsement of LE Proposal;

- LE Session – LE presents case studies on DNS abuse and how LE Proposal would help reduce DNS abuse; session would be open to public in coordination with ICANN staff

- GNSO, ccNSO, SSAC – Advocate LE Proposal thorough ICANN internal organizations - GNSO, ccNSO and SSAC

Action Plan - RIRs

- Join your respective LE/Government Working Group
- Sponsor and support IPv6 Global Policy
  - Finalize draft of IPv6 Policy
  - Ensure your respective RIR has introduced IPv6 E-Crime Policy
  - Attend your next RIR WG meeting and RIR General Meeting
    - AfriNIC – Kigali, Rwanda, June 1-4, 2010
    - ARIN – Toronto, Canada, April 18-20, 2010
    - APNIC – Bankok, Thailand, August 26-30, 2010
    - LACNIC – Curacao, Netherlands Antilles, May 25-30, 2010
    - RIPE NCC – May 5-10, 2010, Prague, Czech Republic


Questions ?