

# NATIONAL RESILIENCE EXTRANET



PREPARING FOR EMERGENCIES



# NRE BACKGROUND

- Stemmed from requests to fund local extranets
  - Secure environment
  - Share multi-agency documentation
  - Lots of applications for funding
- Cabinet Office decided to fund a national extranet
  - Requirement to store and manage **RESTRICTED** information
  - Create areas for local, regional and national levels
  - Provide a “**one view for all**” information picture
  - Enhance communication and **multi-agency interoperability**
  - **Web based**, fully resilient and managed service
  - Contract awarded to BT and UED in Sept 2008

**NATIONAL RESILIENCE EXTRANET**



PREPARING FOR EMERGENCIES

# WHO IS IT FOR?

All responders classed under the CCA04

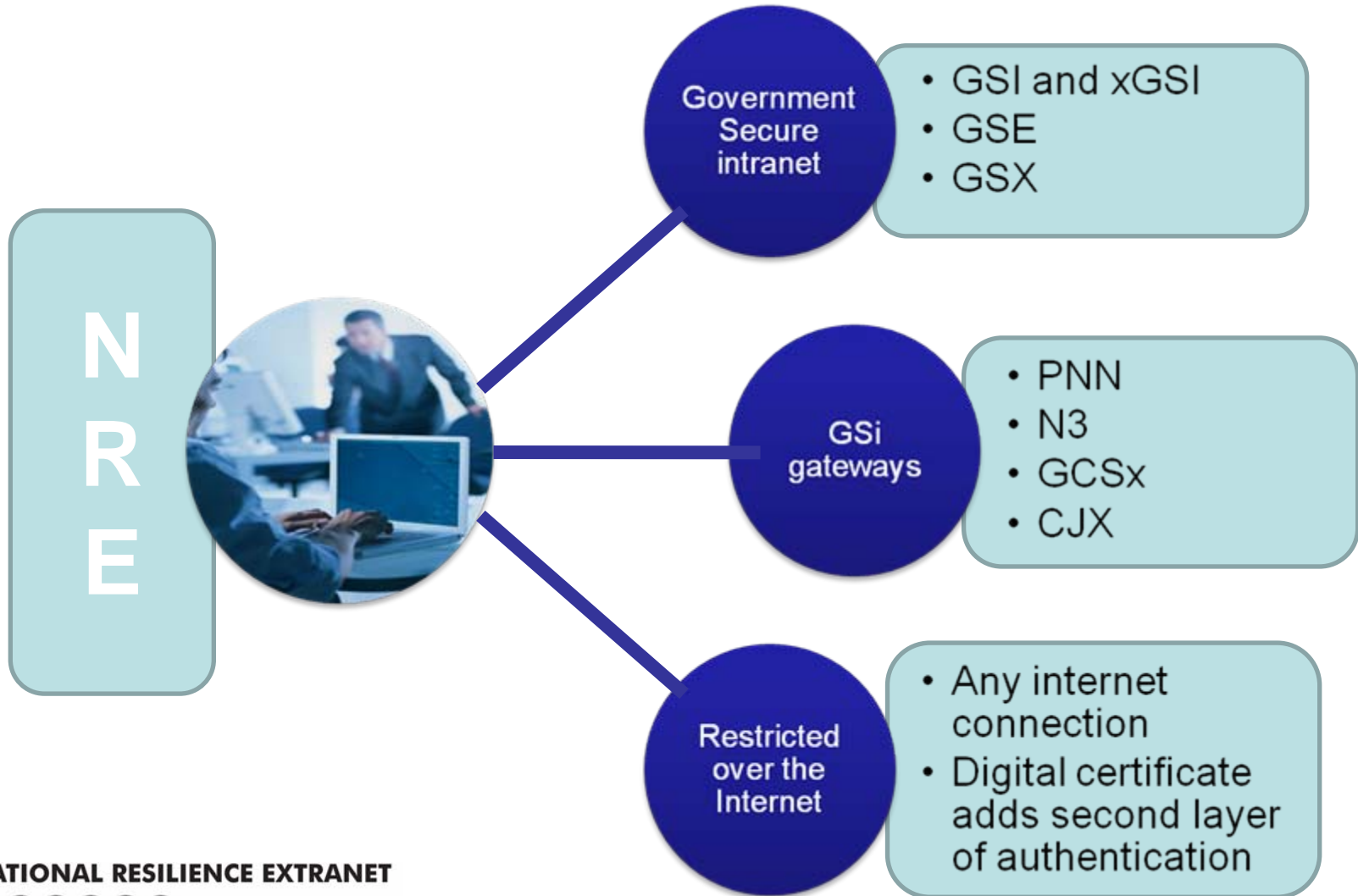
Central  
Government  
Departments

Category 1 & 2  
Responders

Voluntary Sector  
and Private  
Sector who assist

- Designed for 12,000 users
  - 6,000 concurrent users
  - System will be scalable if required

# HOW DO I CONNECT?



**NATIONAL RESILIENCE EXTRANET**



PREPARING FOR EMERGENCIES

# HOW SECURE IS IT?

- Runs on GSi accredited networks
- PKI certificate for use on ROTI access
- Syntaxis architecture and secure gateways used by MoD
  - CESG approved
  - IA&S (formally CSIA) within Cabinet Office
- Document / File security:
  - can be made available to the whole community
  - or locked down to a specific organisation, work group or user(s)
  - further restricted to read only if required
  - full audit trail of who accesses what and when
  - all files scanned when uploaded for viruses / malware
  - synchronous back up to geographically separate DR site

# WHAT AM I BUYING?

- Atlas COLLABORATE
- Day to day planning and information sharing tool
- Fully managed service (99.6% availability)
- Browser based: supported on IE 6 and 7 or FF1.5 >
- £85 per user per annum

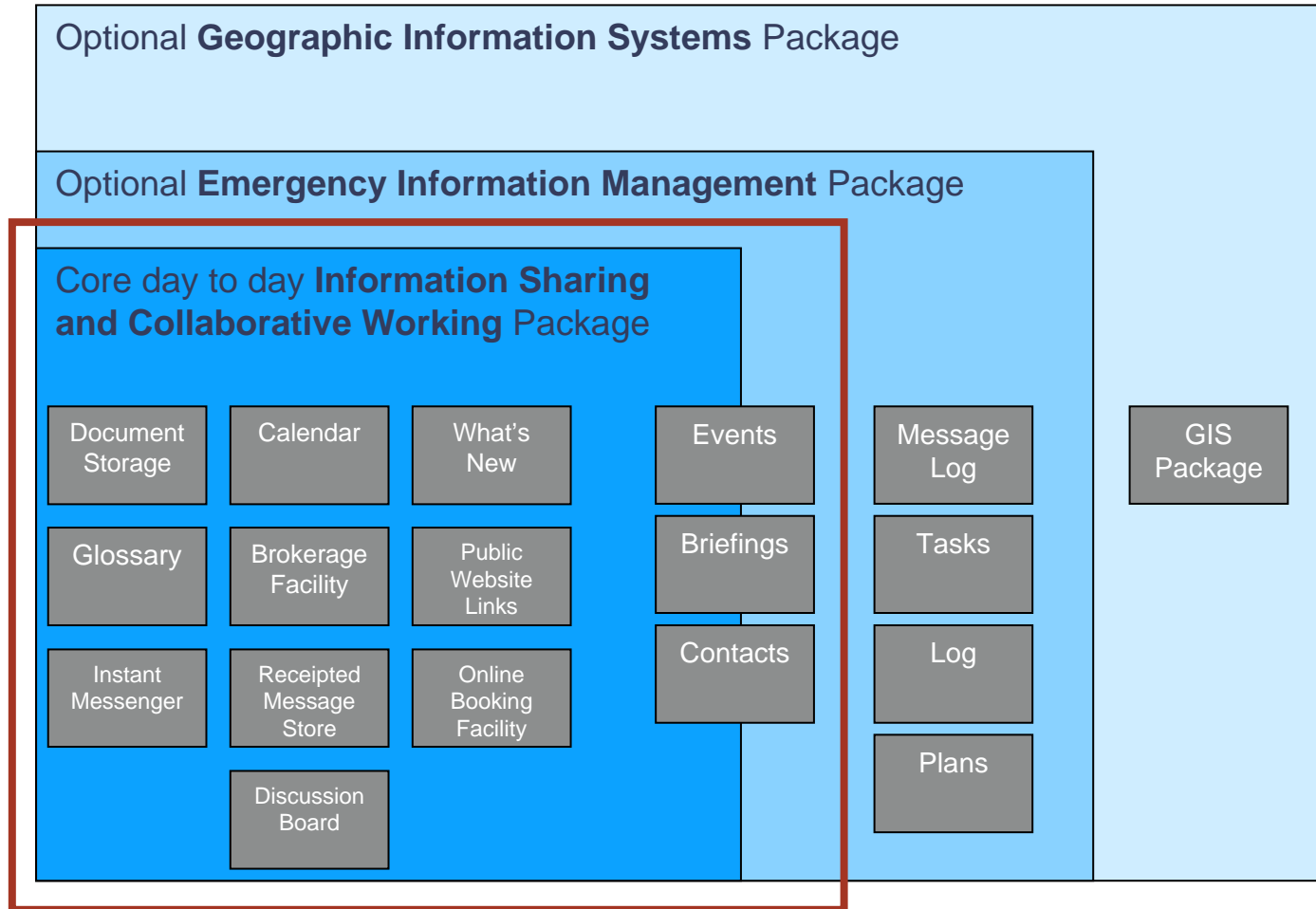
## Optional:

**Atlas AIMS**  
(incident  
management  
system)

**Atlas LT**  
(lightweight  
mapping tool)

**Atlas OPS**  
(mapping tool  
with  
increased  
functionality)

# NRE INTEGRATED SOLUTIONS



**NATIONAL RESILIENCE EXTRANET**



PREPARING FOR EMERGENCIES

# IMPLEMENTATION AT LRF LEVEL

- All organisations need to join for effective collaborative working
- One organisation needs to take the lead
  - Encourage the others
  - Manage the LRF as a workgroup
- Canvass all organisation for take up
  - Some might already be on e.g. EA or Ambulance
  - Minimum of two per organisation for resilience?
- Attempt to gain funding commitment early on

# BENEFITS OF LRF IMPLEMENTATION

- Major Incidents have accurate, up to date information available to all Partners
  - all required participants fully and electronically engaged.
- All reference information required will be held and updated in one secure place
- Information up to RESTRICTED level will be transferable electronically between all Partners for the first time.
- Solution will be run completely as a managed service
  - increased reliability and resilience
  - disaster recovery performance
  - ensure all applications are current.

**NATIONAL RESILIENCE EXTRANET**



PREPARING FOR EMERGENCIES

# SUCCESS AT THE LRF LEVEL

- All identified partners subscribe to at least the minimum agreed licence requirements for the solution to be practically usable by their organisation.
- Each organisation has at least one lead officer (Sponsor) who is trained and able to use the system.
- Staff identified as Sponsors and Local Administrators receive classroom based training from Datel and cascade this learning down to other users within the organisation.
- Start to use the system effectively...

# COLLABORATE TRAINING

- Classroom based:
  - Sponsors (which are super users)
  - Local Administrators - manage the workgroups
  - Train the trainer (train a “standard” user in 30 mins)
  - Go to Datel’s site or Datel will come to you
- Syllabus:
  - One day
  - How to use the system both functionally and procedurally

# SERVICE SPECIFICATION

- Formerly the Code of Connection:
  - to be signed by Organisations CEOs or Senior Officer or equivalent
    - Reviewed on a regular basis
    - Available to view on-line from end of October 09
  - Outlines responsibility for:
    - Staff clearances (BPSS as a minimum)
    - Actions on staff misuse of NRE
    - Sponsorship of organisation outside of CCA
    - Procedures for duty officer log-ins (role based)

# CODE OF PRACTICE

- Also known as an End User Security Agreement:
  - To be issued to each user
    - Outline responsibilities for use of NRE
    - Username, password
    - What level of documents can be added
    - Granting access to information
  - Handling requirements for information held
    - Restricted, protect, unclassified or personal
    - Covers both electronic and hard copy
    - Acceptable types of computers used

# FREEDOM ON INFORMATION

- To be confirmed early November 2009 after consultation with MoJ Security Services FOI specialist.

# DATA PROTECTION

- Any personal data must be:
  - fairly and lawfully processed
  - processed for specified purposes
  - adequate, relevant and not excessive
  - accurate
  - kept securely
  - kept for no longer than is necessary
  - processed in line with the individual's rights
- Obligation is both on the Suppliers and the Subscribers

# ROADMAP

- **October**
  - Continued system development and testing
- **November**
  - Final testing of the system by the suppliers
  - Training can commence in the last week
- **December**
  - UAT 7<sup>th</sup> – 11<sup>th</sup> December
- **January**
  - Phased roll-out to a controlled group
  - Pilots

# NATIONAL RESILIENCE EXTRANET



PREPARING FOR EMERGENCIES

*Questions???*



Working together to deliver the NRE