ContactPoint

Project Board

31 Jan 08

Every Child Matters
Change For Children

ContactPoint
because every child matters

ContactPoint Security Review – Basis of response

- Welcome Deloitte's thorough review and their recognition of the way security is ingrained in all aspects of the team's work
- Demonstrate that the project is proactively managing the high level risks
- Respond positively to the high level recommendations, showing action plans to respond on each point, but without revealing specific implementation or control details
- Rapid impact assessment of the detailed recommendations

- Maintain robust line on main body of the report, that it is not appropriate to reveal this (e.g. under FOI request) as it contains details of identified risks and recommended controls which could be used to attack the system

Response to High Level Risks

- Information might be used to target criminal activity against children at risk…
- ContactPoint project has previously highlighted and is proactively managing the risk of personal information on children falling into the wrong hands by implementing tight access controls, based on strong authentication, and multi-layer security controls, based on best practice standards including ISO27001. We welcome the positive recommendations resulting from this review, which will help further improve these controls.
- Possibility of long-term identity integrity attacks…
- ContactPoint data will never (and cannot by law) be shared with other government data systems. Any discrepancies in child identity data will be referred to the data owner for resolution, to ensure that the data is as robust as possible. As well as ensuring that ContactPoint complies with Data Protection best practice, this will ensure that any integrity attacks come to the attention of the data owner and are investigated.

Response to High Level Recommendations (1)

- Clear communication of responsibilities and accountabilities to LAs and Partners…
- **We recognise the need for this, and we are developing a comprehensive programme of Training, Readiness Assessments and Accreditation checks to ensure these organisations are properly prepared for these responsibilities. The review has identified a number of areas which will be critical to get right as these plans develop. We welcome this advice and will follow it as we finalise our plans.**
- Formal assurance of technical and procedural controls…
- **Government guidance on risk assessment and security controls has evolved significantly since the ContactPoint system was first designed, especially with the release of the new Manual of Protective Security in August 2007. The design is currently undergoing a re-baselining exercise. Once this is complete, we will fully update the risk assessment against the new criteria and initiate a formal, external assessment to ensure these risks are effectively controlled. The scope of this will include the self-certification and LDQT process concerns highlighted by the review.**
- **Further controls over access to central system data**
- **Deloitte has proposed three possible approaches to enhancing these controls. The ContactPoint project will undertake a rapid impact assessment to determine which approach will be most effective in our specific context; and will build this into the deployment plan.**

Response to High Level Recommendations (2)

- **Define processes for secure disposal of electronic and hard-copy media…**
- **Temporary guidance was issued to ensure secure storage and/or disposal of media used for Initial Data Load. This was effective at the time, and will be reviewed against latest government-wide best practice standards to inform standards for production processes. These additional controls will be in place before any data is loaded into the User Acceptance Test or Live systems. The Live system will also be designed to minimise and, where possible eliminate the use of physical media.**
- **Clear guidance on information security matters for helpdesk staff…**
- **The Deloitte review has highlighted one occasion where helpdesk guidance did not reflect best security practice. Formal helpdesk training has not yet taken place, and training plans will be reviewed to ensure that helpdesk staff are aware of security best practice, including the areas highlighted by the review.**
- **Participation in government-wide security initiatives**
- **DCSF is participating in these initiatives, especially those focussed on data security, privacy and strong user authentication. We will take into account all best practice guidelines arising from this work to keep ContactPoint at the leading edge of security practice.**

Security Assessment - handling

- Final report due – 1 February
- Draft submission for David Bell to send to Ministers – by 4 Feb
- Sub from David Bell to(1) Kevin Brennan and (2) S of S – by 6 Feb
- Kevin Brennan asked for a meeting – on 7 February
- Final decision expected from S of S – by 14 February
- Publication – w/b 18 February (press office to confirm date)
  - Summary of recommendations and Govt response on ECM website and LARA
  - Working with NPs and ADCS to support us
- At the same time, announce: timetable, milestones and grant letters