IAAC Identity Assurance Programme 2007
Report of IAAC's 16 October 2007 Workshop
"How UK Government can Gain Citizen Support"

Summary

IAAC held the second of a series of two workshops on the 16th October 2007 to address what UK Government can do to gain the support of its citizens for its national digital identity infrastructure (NDII) plans. The first of the two workshops (4th September 2007) identified the citizen's concerns with regard to the development of an NDII, and the reassurances and support people need if they are to have the confidence to engage with the new infrastructure. The 16th October workshop addressed what UK Government can do to provide those reassurances and support. This paper is a report of the key messages and main ideas which emerged from the 16th October 2007 workshop.

UK Government should ensure that all aspects of its NDII development plans are geared towards building citizen confidence and ensuring the citizen remains safe. It must ensure its approach is open and transparent throughout. It must understand fully the implications its plans might have on the UK's future digital society and ensure it does not build an infrastructure and capability antithetical to the type of society citizens desire. In addition, it should identify any unwanted particular effects its plans might engender and ensure it sets its policies so all such effects are avoided.

It must publicise its proposed identity assurance governance arrangements and put them forward for wide discussion and agreement. It must then put the agreed governance arrangements in place as soon as possible. It must ensure its designs are extremely robust, especially given that the NDII is expected to become a national infrastructure encompassing many millions of identity subjects. It must ensure it builds in strong safety nets for when things do go wrong, and provides citizen control so individuals can take whatever steps they deem necessary to ensure their own safety.

A summarised version of this report is available as IAAC Briefing Paper 66. A summarised version of the report from the 4th September 2007 workshop is available as IAAC Briefing Paper 65.

Background

IAAC's research programme for the second half of 2007 followed on from its publication in 2006 of its Roadmap for Identity Assurance in the UK (the Roadmap) plus the work it conducted in the first half of 2007 focussing on the UK Government's role in creating assured digital identities. Please refer to the report of the 4th September 2007 workshop if more detail relating to this previous work is desired.

That previous work identified several critical goals which UK Government needs to achieve if its NDII plans and developments are to be successful. The most immediate of these was for UK Government to ensure that any developments it undertakes are acceptable to the citizenry of the UK and win the citizen's trust and confidence. This goal was carried forward as the central theme for IAAC's subsequent work in the second half of 2007.

That subsequent work took the form of two workshops which IAAC ran in the Autumn of 2007, the first on the 4th September and the second on the 16th October. The 4th September workshop, entitled "Examining the Needs and Concerns of the Citizen", had as its objective to understand the key concerns of the citizen, and the reassurances and support the citizen needs if people are to have confidence in the Government's NDII plans. The findings of that workshop are contained in a separate report and are summarised in IAAC Briefing Paper 65.

The 16th October workshop, entitled "How UK Government can Gain Citizen Support ", had as its objective to identify what Government could do to provide the reassurances and support the preceding workshop had shown were needed. This latter workshop produced a clear understanding of the approach UK Government should take if it is to ensure citizen confidence. Its findings are the subject of this report and are summarised in IAAC Briefing Paper 66.

Workshop Results

Key Messages

The key messages which emerged from the 16th October 2007 workshop were:

- To create a national digital identity infrastructure which citizens would elect freely to use, UK Government will have to make building citizen confidence and ensuring citizen safety central priorities for each and every aspect of the approach it follows.
- UK Government must ensure that the NDII which emerges as a result of its plans supports and strengthens, rather than hobbles or burdens, the future UK digital society. It must ensure it understands how its plans might influence, lead to, or drive changes in the characteristics of that future society, and must ensure that none of those changes would undermine, or be antithetical to, the desired characteristics of the society it is trying to strengthen, support and protect.
- UK Government must look not only to the possible benefits an NDII might provide but also to the possible unwanted effects its NDII might engender, and it must set its policies to ensure all such unwanted effects are avoided. UK Government must ensure its plans do not inadvertently lead to the creation of powerful new capabilities which extend beyond current needs and which are then at risk of being misused by a future government.
- To build and sustain citizen confidence, UK Government should be open about its NDII goals and strategy and should be transparent in all aspects of its NDII plans and developments.
- UK Government must develop comprehensive identity assurance governance arrangements geared around building citizen confidence and ensuring the citizen remains safe. It should ensure its proposed governance arrangements are widely debated and agreed, and should move quickly to put the governance arrangements in place as soon as possible, not just "in due course".
- A key design goal is for the NDII to provide citizen control. This should include the ability for the citizen to reduce their involvement with the NDII to a minimum if they feel it necessary for their own safety.
- As found in the 4th September workshop, there is a general distrust of government's ability to deliver and operate complex systems. UK Government must strengthen its information management culture and raise its data security performance if people are to have confidence in its ability to run information-intensive infrastructures reliably, safely and securely.

Findings

The following are the ideas which emerged from the 16th October 2007 workshop.

Achievable Goal

The results of the IAAC workshop of the 4th September provide the starting point from which UK Government can identify the things it needs to do to gain citizen support. In summary, that preceding workshop showed that citizens have a number of very substantial needs and concerns which will have to be addressed if citizens are to acquire the confidence to engage with new digital identity infrastructure. There are real risks to the citizen associated with the development of an NDII, ways, which people do not yet understand, in which things can go wrong and people could be harmed. People do expect that the NDII should be made safe for them to use, but do not yet know what sorts of protections and safeguards to ask for. They do have doubts about the extent of Government's intentions to protect its citizens' interests and about its competence to run information-intensive infrastructure safely, so will insist on having sufficient control themselves so they can ensure their own safety.

Government will have a challenge to address all these needs and concerns. However, it can remain confident it should be able to create a national digital identity infrastructure which citizens would elect freely to use. To achieve that, though, UK Government will have to make building citizen confidence and ensuring citizen safety central priorities for each and every aspect of the approach it follows.

Road transport serves as a useful analogy here. As well as giving UK Government confidence that its goal is achievable, it provides an indication of some of the powers and safeguards which go towards making an infrastructure of this nature safe enough people will be willing to use it.

The UK's road transport infrastructure provides benefits people want without putting the citizen at undue risk.

- The country's road transport infrastructure plays an essential role in many many aspects of an individual's daily life. Imagine the encumbrance if the UK had a fragmented road infrastructure;
- There are serious harms which can befall people using the roads but this does not stop most people from engaging with the road transport infrastructure on a regular daily basis;
- People feel they understand the dangers of driving and the personal risks involved. They are able to make their own choices regarding the degree and manner to which they use the infrastructure to ensure their own safety and protect themselves;
- Confidence has matured into trust. People have learned they can trust the protection mechanisms built in to the infrastructure (e.g. the availability of sufficient road signs, the correct functioning of traffic lights, the restraints on other road users' behaviours).

This infrastructure is supported by effective and efficient safeguards and protective arrangements:

- Safety is a priority in the design of both the infrastructure itself and the means by which other people use the infrastructure (cars, public vehicles);
- There are clear codes of behaviour for all who use the infrastructure, backed by licensing, continual monitoring of user behaviour, and an effective enforcement mechanism which applies to all users equally;
- There is ample immediate and independent public reporting of major and minor disasters.
- Appropriate arrangements come into play whenever things go wrong (e.g., prompt response by the emergency services, the closing of roads following a major accident).

Understanding the Implications of its NDII Plans

To ensure the development of an NDII supports and strengthens, rather than hobbles or burdens, the future health and wellbeing of the UK digital society, UK Government must ensure it understands how its plans might influence, lead to, or drive changes in the characteristics of that future society. It must then make sure that none of those changes would undermine, or be at odds with, the desired characteristics of the society it is trying to strengthen, support and protect.. Any NDII developments should maintain "contextual integrity". That is, UK Government should take care not to introduce or require attitudes, approaches or conduct which are not normal or fitting within the social or societal context. For example, Government should avoid broaching or pervert the normal relationship between citizen and state.

- Can the goal of improving the delivery of services by taking them on-line lead anywhere other than to a decrease in privacy through the wider sharing of data and the greater mining of a wide range of databases to aid the detection of fraud? Are citizen's prepared to forego this slice of their privacy?

- There are some information-intensive services (e.g. ANPR – Automatic Number Plate Recognition) which serve the public good and can provide greater equity but do so at the expense of increased surveillance. Is this acceptable or is it a step too far?
- With regards to anonymity, the default in the physical world is that a person is anonymous (though identifiable) until there is a need for the person to be identified. The default developing in the on-line world appears to be different. It is for people to be identified much more readily and for a much wider range of activities, including those for which people do not normally need to be identified in the physical world. Are citizen's willing to accept this change?
- We appear to be moving in a direction where the level of trust between citizen and government has been eroded. Not only do citizens now seem to trust their Government less than in the past, NDII developments, including the ID Cards bill, give the impression that government no longer trusts its citizens. Is this interpretation correct? Is the erosion of trust inevitable or of little consequence? Can further development of an NDII do other than accelerate society's movement in possibly an unwanted direction?

Policy Approach

UK Government must look not only to the possible benefits an NDII might provide but also to the possible unwanted effects an NDII might engender, and it must set its policies to ensure all such unwanted effects are avoided. UK Government should strive to ensure its plans do not inadvertently lead to the creation of powerful new capabilities which extend beyond current needs and which are then at risk of being misused by a future government.

UK Government's policy approach should be formed not only on the basis of achieving desired benefits (mission-based policy formation) but also on the basis of avoiding unwanted effects (effects-based policy formation). Mission-based and effects-based policy formation can lead to widely different policy decisions, and decisions regarding the development of national infrastructure affecting citizens' daily lives should be judged on the basis of both the desired benefits and the unwanted effects. Situations do arise, and the NDII might well be one, where technically feasible and potentially highly beneficial capabilities should remain undeveloped if the consequential effects are judged sufficiently undesirable or inappropriate.

In areas such as the creation of an NDII where the adverse effects can be considerable, effects-based policy has an advantage in that it makes more likely a full discussion of all the possible adverse effects an initiative might have. For an NDII, an effects-based policy approach would consider explicitly effects such as the difficulty of recovering a compromised identity and ensure the infrastructure's design includes full and effective response, restitution and redress capabilities. It would also lead to the creation of records of the effects considered and the judgements and decisions made, valuable for later review and accountability.

There would be enormous benefit in the development of a set of ethical principles which would provide guidance to the well-intentioned policy maker to help them avoid developing capabilities which might have unacceptable effects or have effects which should at least be considered most carefully. Such principles would help UK Government ensure its plans do not inadvertently lead to the creation of powerful new capabilities which extend beyond current needs and which are then at risk of being misused by a future government.

Development Strategies

Regardless of the particular requirements around which the NDII is designed, the approach UK Government adopts has to be designed to engender citizen confidence. An essential aspect of that is openness and transparency, and UK Government should be open and transparent in all aspects of its thinking and NDII development. Without these, people will feel threatened by Government's plans and will not have confidence their interests, rights and safety are being protected.

- UK Government should be open about its NDII purposes and strategy. As established in the preceding workshop, people need to know the Government's purposes for creating an NDII. The particular purposes it has in mind will have a significant impact on the nature and form the resultant NDII will take (e.g. affecting whether citizen participation is mandatory or optional).

- UK Government should develop its identity assurance governance arrangements openly and these should put the protection of the citizen as identity subject at their centre. The proposed governance arrangements should be widely discussed and debated so citizens can not only understand their responsibilities within the NDII but also participate in agreeing the restraints to be imposed on how the NDII is to be used, plus other aspects of how their interest are to be protected.
- UK Government should move quickly to put the agreed identity assurance governance arrangements in place as soon as possible, not just "in due course" (as was proposed in its Transformational Government strategy of 2005). As part of those arrangements, the NDII Commissioner (or equivalent) should be appointed as soon as possible and not just prior to the start of operation.

Infrastructure Designs

As with its policy and strategic approaches, UK Government must ensure its designs focus on building citizen confidence and ensuring citizen safety. Its three primary objectives should be:

- To make sure that all opportunities for failures and errors are minimised;
- To ensure there are strong safety nets in place to arrest problems when they occur and to provide satisfactory restitution and redress;
- To ensure it provides sufficient citizen control.

Minimise Opportunities for Failures and Errors

UK Government must ensure its protections against failures and errors are very highly effective. This is especially important given the expected scale of the NDII (with the number of identity subjects potentially being in the millions) and the bringing together of essential identity assets into one infrastructure (which creates a very highly critical piece of infrastructure). If people start to expect that they themselves are likely to experience problems first hand, or they find that other people they know get directly affected by something going wrong, the level of protection they will require in order to feel their continued engagement is safe will take a sizeable leap upwards.

Key areas to be covered include:

- **Identity Subject Enrolment**. The enrolment process introduces huge design challenges. The process needs to be local and convenient for people across the entire country and across a diverse population of millions. It also needs to be robust so identity subjects and reliant users can have confidence in the authenticity and correctness of the digital identities created and the associated data held. Government cannot use the existing data it holds about citizens to create the foundation for enrolment in the new infrastructure as that data is far too inaccurate and incomplete. The enrolment processes must include adequate checks to prove the accuracy and authenticity of the data gathered at the enrolment stage, backed up by continual checks over time to identify and weed out poor quality data.
- **Data Maintenance**. Data maintenance is an even more challenging issue than initial data capture. Updating and correcting a broad spread of data relating to the identity subject correctly and in a timely manner whilst preventing fraudulent or erroneous updates will introduce additional and substantial challenges of its own.
- **The Protection of Biometric Data**. People are particularly concerned that biometric data should be very strongly protected from misuse. They feel biometric data is deeply personal and can be used against them in ways they do not understand.
- **Restricting Data Access**. As strong safeguards to control access to information are built into the systems which comprise or use the NDII, UK Government will also need to ensure that alternative,

less well controlled, channels to the same or similar data are closed off. Relying service providers should not be able to acquire the information they need about a subject or perform the identity checks they seek through other less controlled or restricted legacy systems (e.g. insurance databases).

Put Strong Safety Nets in Place

UK Government must ensure there are strong safety nets in place to arrest problems when they occur and to provide satisfactory restitution and redress. The essential role of safety nets in enabling citizen confidence was made clear in the preceding workshop. Developing an identity infrastructure under which essential identity assets are brought together into one system can make recovery from failure very difficult, as it reduces the opportunity to go outside the system in order to recover from failures. UK Government must ensure it makes extensive provision for response, restitution and redress.

Key areas to be covered include:

- **Identity Repair**. Identity repair is a very challenging issue as it is not immediately clear how a broken digital identity would be repaired. The options and processes for the recovery of a compromised identity must be developed very thoroughly, not just on a "best efforts" basis.

- **Redundancy and Contingency Arrangements**. When something goes wrong within the NDII, the Government will be expected to close that part of the infrastructure involved and ensures it stays closed until any root causes have been resolved. Government will need to design in redundancy and contingency arrangements so people can continue to access services and go about the activities of life without being significantly inconvenienced as a result.

- **Consequential Effects**. If the NDII becomes an essential piece of core infrastructure for relying systems, the consequential disruption caused by infrastructure failure could take any of a wide variety of forms. Hence, relying systems as well as the core infrastructure will need to contain contingency for infrastructure failure. What would the contingency response be if a central identity system were to go down just as someone is trying to access an important service? "Come back next week" would hardly be a satisfactory answer.

- **Legal structures**. There is a pressing need for legislation, policing and the justice system to catch up with the realities of the information age. Some aspects of legislation are based on out of date models of the way the world works and the capabilities technology enables. For example, protections contained within the Data Protection Act pertain to data where the individual can be identified explicitly. With today's powerful data matching and profiling capabilities, explicit identifiers are not always needed in order for people to be identifiable from aggregated data. There is a need for stronger data and citizen protection obligations, for updating and strengthening the powers of the ICO and the penalties for breaches, and for making the public sector subject to the same restraints as the private sector.

Provide Citizen Control

A key design goal is that the NDII must provide citizen control. As identified in the preceding workshop, while people have doubts about the fullness of the government's intention and ability to protect their interests, they need to have the ability to take whatever steps they deem necessary to keep themselves safe.

- People must have the option to "opt down". That is, even if it is not practicable for someone to "opt out", to refuse to engage with the NDII entirely, they must at least have a real ability to scale their engagement down to a minimum level at which they feel the remaining dangers of their continued engagement are no longer too high. Any disadvantages from opting down, such as slower access to services, must be reasonable consequences of their chosen degree of disengagement and must not lead to disenfranchisement.

- Choice needs to be informed and genuine, not an unfair prerequisite for access to a basic benefit or entitlement.

- People must be able to enforce restrictions on what personal data is held about them by whom and the uses to which that data may be put. People recognise that their personal data can be used in powerful ways, not always in their own best interests.

In addition, the assurance process the Government utilises must be suitable for the task.

- UK Government is expected to be conducting system assurance and accreditation under the approach it has used for other large complex projects. Given the unique nature of the development of an NDII and of the citizen as stakeholder, UK Government should review whether that approach has the power to address the risk challenges of the NDII.
- Normal system assurance does not assess the suitability of the decision to go ahead with a development, it takes that decision as closed. For the NDII, assurance should bring that decision within the scope of review and cover all the possibly unwanted effects the infrastructure might have. Further, the NDII commissioner should be able to review and report on the design process and the resultant design, not just on the operation of the infrastructure once built.
- External and open reviews of infrastructure designs are recommended, to ensure the comprehensive identification of safeguards and to aid citizen confidence.

Operation

As found in the 4th September workshop. there is general scepticism regarding government's ability to operate complex systems reliably, safely and securely. UK Government will have to work to strengthen its information management culture and raise its data security performance if people are to have confidence in its ability to run information-intensive infrastructures well.

- The FoIA has brought to light that many areas of government still have poor information management cultures and practices. Evidence suggests that the FoIA is often seen by those subject to it in a negative light, and that officials look for opportunities to avoid some of the restraints or requirements associated with FoI requests and responses.
- Operational security breaches seem to arise continually and from a whole variety of sources. Government has to rectify its current data security shortcomings immediately, take a very firm line against those who commit security breaches with personal data, and convince the public it has these problems under control.

Government officials are not the only ones to practice poor information management standards, and Government will have a job to ensure there are few opportunities for the citizen themselves to cause operational failings. People still fall for phishing attacks and display very low levels of security common sense. Government cannot rely on the average member of the public to be aware, informed, or to act securely, and will need continually to broadcast fundamental safety and security messages.