The Disclosure and Barring Programme: Privacy Impact Assessment (PIA)

Version: 0.5

Date: 20 December 2012

Author: Chris MacLeod

Owner: Jackie Sear

Synopsis:	Privacy Impact Assessment (PIA) conducted on the Disclosure and Barring Programme
Document Status:	Draft
Document Name:	DBP Covering PIA v0.5

Document Location

Corporate File Plan (F:_CFP\1-Crim Red\11-Sptg Svcs\012-DBP\05-Bus Case\03-FBC\02-Res\01-Docs)

Document History

Description/Reason for Change	Author	Version	Type of Review	Date
First Draft	Jackie Sear	0.1	Initial draft	10/08/12
Update	Chris MacLeod	0.2	Updating	12/11/12
Adding detail from supporting PIAs	Chris MacLeod	0.3	Formal 5 day	04/12/12
Update following Formal 5 day review	Chris MacLeod	0.4	Formal 2 day	14/12/12
Update following Formal 2 day review	Chris MacLeod	0.5	Programme Board	20/12/12

Approvers *(those who have final authority to approve the product)*

No.	Name	Organisation/Role	Version	Issue Status
01	Jackie Sear	DB Programme Manager	0.5	
02	Disclosure and Barring Programme Board	Disclosure and Barring Programme Board	0.5	

References/Related Products

No.	Document / Material	Location (CFP location Reference)
01	DBS Go-Live PIA Final v1 0 2012-11-27	F:_CFP\1-Crim Red\11-Sptg Svcs\012-DBP\05-Bus Case\03-FBC\02-Res\01-Docs
02	DBS Outsourcing PIA v1_1	F:_CFP\1-Crim Red\11-Sptg Svcs\012-DBP\05-Bus Case\03-FBC\02-Res\01-Docs
03	ISA CRB NPIA PIA v0.4	F:_CFP\1-Crim Red\11-Sptg Svcs\012-DBP\05-Bus Case\03-FBC\02-Res\01-Docs
04	ISA TA GTC WA v1.0	F:_CFP\1-Crim Red\11-Sptg Svcs\012-DBP\05-Bus Case\03-FBC\02-Res\01-Docs
05	Update_Service_PIA_v1.0	F:_CFP\1-Crim Red\11-Sptg Svcs\012-DBP\05-Bus Case\03-FBC\02-Res\01-Docs

Disclosure and Barring Programme – Privacy Impact Assessment

1. Introduction and Overview

1.1 This is an overarching Privacy Impact Assessment on the Disclosure and Barring Programme (DBP). It sets out the purpose of the Programme and its relationship to Home Office business, how the Programme is structured and the individual PIAs that have been prepared. This PIA contains information from the individual PIAs.

2. The DBP - Purpose and its relationship to Home Office business

2.1 The Programme for Government Coalition Agreement included a commitment to scale back the disclosure and barring services currently delivered by the Disclosure and Barring Service (DBS), but formerly by the Criminal Records Bureau (CRB) and the Independent Safeguarding Authority (ISA), to "common sense levels." In fulfilling this commitment, the Government will deliver the following improvements to disclosure and barring services ensuring they:

- are **efficient and easy to use**, removing unnecessary burdens for employers, employees and those who volunteer;
- are **more proportionate** and better protect the rights of the individual; and
- help to **safeguard children and vulnerable adults** from abuse by those who work with them.

2.2 The Government commissioned **Reviews of the Vetting and Barring Scheme (VBS)** and of the **Criminal Records Regime (CRR)** to consider in detail how to deliver these improvements. The Reviews reported in February 2011. Both reviews include a range of recommendations that will collectively deliver the improvements identified above. Key recommendations include:

- a barring function, currently carried out by the Independent Safeguarding Authority (ISA) that would be retained, but with reduced coverage;
- registration and monitoring would be scrapped – under the previous plans 9.3m individuals working with children and vulnerable adults would have been required to register for monitoring;
- a new portable disclosure service would be developed for individuals, employers and voluntary bodies; and
- the merger of the CRB and the ISA which will be replaced with a single new organisation, the Disclosure and Barring Service (DBS) which will be responsible for delivery of the disclosure and barring functions;

2.3 The Disclosure and Barring Programme (DBP) has been established to implement these Review recommendations and, as a result, to deliver the Government's vision for disclosure and barring services, as described above. The Programme has now delivered the new organisation, the DBS. References to the former CRB and ISA are reflected by specific reference to the Disclosure or Barring arms of the DBS or either of its locations. The Programme is Home

Office-led and delivered in partnership with a range of key stakeholders, most notably the Department for Education, Department of Health and the DBS as well as colleagues from the devolved administrations in Scotland, Wales and Northern Ireland. The Programme Team comprises people drawn from Home Office and DBS.

2.4 The net result of this policy change is to restore public faith in disclosure and barring services by making this a more proportionate and less burdensome process, whilst contributing to effective public protection arrangements; and making them more proportionate and effective in order to deliver the Government's published aim of scaling the criminal records regime back to common sense levels. These changes will strike the right balance between civil liberties and public protection.

2.5 The Programme was structured to deliver through two projects, the DBS Project and the Update Service Project along with a number of workstreams: Business Case and Benefits; Policy and Legislation; Requirements; Commercial; HOIT On Boarding; Stakeholder Engagement and Communications; Transition and ICT; and 'September 10th legislative changes'. A summary of these projects and workstreams is as follows:

3. DBS Project

3.1 The DBS Project was the dedicated project with responsibilities that included the delivery of the enabler processes and tools, e.g. transfer scheme, along with the Board (Chair and members) and Executive Management team (primarily the CEO) necessary for the new body to be vested, quorate and have sufficient preparation ready for transition to a new single organisation (the DBS). This Project was responsible for the recruitment of the new Chair, Board and Chief Executive of the DBS. Alongside the appointment of the CEO of the DBS, this project focused on the planning and delivery of elements essential to make the establishment of the DBS a success and be ready to vest successfully on 15 October 2012.

3.2 This Project worked alongside the CRB and ISA who were responsible for the close down of their respective organisations. The DBS went live on 1 December 2012.

4. The Update Service Project (formerly the CRSC Project)

4.1 The Update Service Project is responsible for the development of the new online portable update service. This builds on the existing disclosure service, transforming it through a small number of key changes to the current disclosure process.

5. The Workstreams

5.1 The Programme also included a number of workstreams responsible for the delivery of key elements of the Programme:

Policy and Legislation: responsible the legislative changes required to implement the reviews through the Protection of Freedoms Act. It will also deliver secondary legislation and any statutory guidance required after the Bill is enacted and develop the policy Route Map.

Requirements: responsible for articulating the outcomes and specifications in terms of the business requirements and maintenance of the Requirements Catalogue.

Transition and ICT: management of the end to end transition from existing contractual arrangements to new arrangements including co-ordination with HOIT On Boarding.

Commercial: responsible for leading the procurement exercise to replace the Business Process Outsourcing and Application Management and Development contracts. The Programme was identified by Cabinet Office as a LEAN pathfinder, designed to cut the time and cost of traditional public sector procurements.

HOIT Onboarding: in line with the wider Home Office ICT strategy, responsible for managing the transition to the HOIT shared service platform, which will include infrastructure, desktop and telephony.

Stakeholder Engagement and Communications: responsible for internal and external communication activity, in particular ensuring that those who use disclosure and barring services understand the changes we are making and how it will affect them.

Business Case and Benefits: responsible for the development and maintenance of the Full Business Case, defining and monitoring the delivery of programme benefits and maintaining accompanying financial models.

September 10th Legislative Changes: responsible for the oversight of the implementation of the early legislative changes in the CRB and ISA.

Of these projects and workstreams, the following remain active within the Programme at present (the remainder having been transferred to the DBS or closing naturally as work completed):

- The Update Service Project
- Transition and ICT Workstream
- Policy and Legislation Workstream
- Business Case and Benefits
- Communications

6. Awareness, Scoping and Impacts

6.1 Supporting PIAs

6.1.1 Six separate PIAs support this overall Programme PIA:

Procurement/Off-shoring: This Privacy Impact Assessment specifically relates to the procurement and outsourcing of the development of a new ICT solution and Business Process Outsourcing contract, with specific focus on the "off-shoring" aspects of the service, including the handling and management of individual's data and the potential privacy risks that this may raise.

This PIA was been drafted and formally reviewed by Programme and DBS colleagues.

Independent Safeguarding Authority (ISA) provision of NPIA data to the CRB: This PIA relates to DBS Barring (formerly the ISA) sharing of NPIA personal information with DBS Disclosure (formerly the CRB). This will enable the DBS Disclosure to undertake a check to verify whether an individual has applied for a Barred List check which is only undertaken where an individual has applied or is applying for work in Regulated Activity.

Independent Safeguarding Authority (ISA) provision of ISA data to TA, GTCW and WA: The disclosure of DBS Barring (formerly the ISA) data to the TA (Teaching Agency), GTCW (General Teaching Council (Wales), and WA (Welsh Assembly) to undertake a match against their own records to ensure appropriate action is taken to protect children and vulnerable adults.

Disclosure and Barring Service Go-Live on 1 December 2012: This PIA builds on the legislative changes and the implications of a combined disclosure and barring service. This PIA sets out the arrangements under which the CRB & ISA previously collected and processed information and how these functions transferred to the DBS. It also relates to the data that will be held by the DBS in order to carry out its statutory functions.

Update Service Go-Live: The Update Service is dependent on the personal data collected via the DBS Disclosure Service (formerly the CRB) and processed by CRM (CRB's legacy system). The Update Service uses much of the functionality of the existing service so it is only the changes and new functionality that were assessed in this PIA.

Transition to the new supplier/new IT system: A PIA will need to be conducted on the various changes that will come into effect following the start of the new contract. This will include the new IT system, Update Service full solution and Barred List checks. Work on this PIA will begin in early 2013 with a view to introducing its relevant aspects into this DBP PIA in Spring 2013.

6.2 Awareness

6.2.1 The DBS operates established processes and systems for the management of sensitive personal information in compliance with HMG standards and practices. The DBS will continue to operate these processes and systems for the management of data.

6.2.2 The CRB and ISA operated established processes and systems for the management of sensitive personal information, incorporating data from the Police National Computer, Local Police Forces and other sources. DBS Liverpool currently operates an "**Online Tracking Service**" allowing applicants to check the status of their disclosure applications. DBS Darlington currently has no direct Web access, although some information is made available to third parties.

6.2.3 A number of sources of evidence are available to demonstrate that the privacy of personal and sensitive information has been taken into account:

1. Security-related **Business Requirements** provided to potential new suppliers during the OJEU process;
2. The Security Standards that the new supplier must conform to;
3. A more detailed coverage of the security requirements;
4. The supplier Terms and Conditions include provisions for audits for the integrity, confidentiality and security of Authority data;
5. The security clarifications provided by the new supplier.

6.2.4 The DB Programme has also carried out an initial Business Impact Assessment (IS1) of data, which assesses Privacy issues, and is using this information to develop the accreditation strategy through a Security Working Group (SWG).

6.2.5 The DBS publishes details of their commitment to be fully compliant with the Data Protection Act 1998 and list the principles that will apply when handling personal data in the DBS Privacy Statement. This statement demonstrates privacy awareness. In addition, the Disclosure application form includes a 'fair processing notice' that explains how an individual's personal data will be used.

6.2.7 The DBS will only hold data about an individual if they have applied for a Disclosure check, applied to be a counter-signatory for a Disclosure check or been referred to the Barring Service.

6.2.8 The DBS is the 'data controller' of all data held within the DBS. This means that the DBS will hold full responsibility for the safety of the data contained on a DBS Disclosure application form and data held on all referrals to the Barring Service once it has been received by the DBS. The DBS will hold full responsibility for all data held within their IT systems.

6.2.9 The DBS Barring arm is required by SVGA, POFA and secondary legislation to provide specific information to the Teaching Agency, General Teaching

Council (Wales) and the Welsh Assembly who regulate their respective professions to ensure children and vulnerable adults are protected from harm.

6.2.10 The DBS have also considered the impact the new Update Service could have on its customers in relation to the Human Rights Act 1998 (HRA). In so doing, consideration has been given to Article 8 (specifically private life) and whether any form of discrimination with regards to Article 14 could also be invoked as a result of that consideration. It was found that the new service would not breach an individual's rights as protected by the ECHR.

6.3 Scoping

6.3.1 DBS Liverpool will only collect and process relevant information to enable it to produce Disclosure Certificates as requested and consented to by the Disclosure Applicant.

6.3.2 DBS Darlington will only collect and process relevant information with regard to safeguarding referrals made to it. This change will enable informed decisions to be made as to whether an individual should be placed in either of the Barred Lists (children or adults), or both.

6.3.3 A number of changes will need to be made as the DB Programme progresses and these include:

1. A change to the handling of sensitive personal data through the introduction of a process whereby a file containing personal and barred status information will be emailed over GSI and CJSM secure networks from the DBS Darlington to the TA, GTCW and WA;
2. Individuals wishing to subscribe to the Update Service online process will be presented with a 'fair processing notice', which the individual must acknowledge before they can complete the process;
3. In order to collect and manage specific historic personal data about transsexual customers subscribing to the new Updates Service appropriately, some adjustments to existing disclosure processes were required. These new processes enable transsexual customers to use the Disclosure service without disclosing details of their previous identity or gender. Such cases will only be considered by a specialist team in the DBS.
4. A new online payment facility will be provided by a third party supplier for customers wishing to join the Update Service. Because this service will give the individual the option to automatically renew their subscription annually, the payment system must be able to retain the individual's payment details.
5. XML files will be transmitted between DBS Darlington and DBS Liverpool using the Government Secure Intranet (GSI) containing Name(s), Aliases, DoB, PNCID and ISA Reference Number. This is an interim solution until a new process with the NPIA is agreed so that they can provide DBS Disclosure with the required information.

6.4 Impacts

6.4.1 The formation of the DBS presents no change in the impact on privacy to individuals as compared with when the CRB and ISA were in existence. There will be no additional collection of data from individuals over and above that already in place currently.

6.4.2 However, a number of potential risks have been identified along with the impact they may have on individuals should they arise:

1. Information could be inappropriately disclosed resulting in a breach of the Data Protection Act and distress or harm to the individual(s) involved;
2. Sensitive personal data relating to transsexual customers (relating to their previous gender) could become known to persons outside the specialist DBS team which could lead to distress or harm to the individual(s) involved. It could also affect the individual's employment prospects and would cause reputational harm to the DBS; and
3. If the Update Service payment system is not secure, there is a risk that customers could suffer financial loss, which could also damage the reputation of the DBS.

6.4.3 A number of measures were established by the CRB & ISA and have been transferred over to the DBS in order to reduce the likelihood and impact of such situations. These measures include:

1. The disclosure and barring process is not open to everyone – it is accessible only to employers in order to use the information to protect children and vulnerable adults;
2. DBS buildings have physical security measures in place to ensure appropriate access/egress;
3. DBS staff are made aware that breaches of the Data Protection Act may result in legal proceedings being brought against them;
4. DBS staff with access to personal data are subject to a minimum of Baseline Personnel Security Standard (BPSS) security clearance;
5. DBS staff are required to undertake annual data protection training;
6. DBS staff access is managed by the RBAC (Role Based Access Controls) process;
7. Access to DBS Customer Management Systems is 'Air Gapped' with no access to the Internet and no remote access; reducing the threat of hacking;
8. All documentation is evaluated and given an appropriate protective marking in line with HMG guidance;
9. Any data exchange takes place over a secure, accredited network or via recorded delivery to defend against interception during file transfer.
10. The Disclosure system has random generated checks to monitor user data browsing;
11. Audit reports can be produced to establish which users have accessed specified disclosure cases; and

12. To maximise the safety of the payment details held by the third party supplier, Capita Payment Services (a division of Capita PLC), for the Update Service, the Programme has ensured that they:
    a. are PCI DSS compliant;
    b. use encrypted keys when capturing payment card details;
    c. use HTTPS when communicating with the CRM.

7. Summary of Privacy Risks and Mitigation

7.1 What are the Privacy Risks relating to the amount/type of data collected?

	Privacy Risk	Mitigation
1	Data interception during transfer of information between DBS and appropriate individuals or organisations	Use of a secure network email exchange for electronic data exchange and via recorded delivery when postal
2	Personal or sensitive data being viewed, used or accessed inappropriately by DBS staff or personnel from the TA, GTCW or WA	• RBAC and Access Assurance checks (Audit) • User awareness training • Minimum BPSS security clearance for all staff
3	Electronic attack on Home Office Network or Customer Management Systems	Security controls in place as per HMG standards
4	Holding sensitive information in a second location i.e. DBS holding information originating from the Police Service	Partially mitigated by the DBS only holding "flagging" information (rather than the information itself)
5	Users (customers) access personal information they are not entitled to access	For website access, application number and date of birth are required to obtain any information on an applicant. The information returned to the user is tracking information (e.g. whether the disclosure status has changed, or the progress of an application). Very limited private information is available through the web site – for instance, the information held on a disclosure certificate is not available via the website.
6	Holding inappropriate information	• Information Sharing Agreements are in place to define what information should be shared with Police and other parties – for Disclosure, all data fields are pre-agreed with the NPIA. • For barring, a wider range of

		information can be held. The existing Barring service process ensures that only appropriate information is held.
7	Information is accidentally released	• The implementation of the new solution will eliminate the holding of new cases in paper format – electronic copies will be more secure and reduce the likelihood of accidental release. • Technical controls in the ICT solution, will improve the security of information.
8	Identity details relating to transsexual applicant's previous identity or gender are released to a third party	• Redirecting system generated notifications arising from the Update Service relating to transsexual individuals to a specialist DBS team • Flagging cases as sensitive • Training staff to refer enquires on sensitive cases to the specialist team • Random generated system checks on user access • Annual training on the Data Protection Act for all staff • Audit logs are generated for all user interactions with customer records on the system
9	Individual's payment details being accidentally disclosed, lost or inappropriately used	• Using a payment service that is level 1 PCI DSS compliant • Use of encrypted keys to protect payment details during the transfer of data between CRM and payment service • Ensuring a secure communications protocol (HTTPS) us used when transferring data between CRM and the payment service

7.2 What are the Privacy Risks relating to the sensitivity and scope of the data collected and how might security controls mitigate them?

7.2.1 For the most part, this is as described in section 7.1 above. However, information collected and managed by the DBS for Barred List and Barring

Case Management which has been identified as being *Highly Sensitive* information with an Impact Level (IL) of IL3 and IL4.

7.2.2 The DB Programme will not alter the collection or management of this highly sensitive information in a manner that alters the existing risk of it being misused or inappropriately accessed. This existing risk is already (and will continue to be) mitigated against by processes that have been developed for the management and distribution of Barred Lists and such information is not accessible to BPO staff, either in the UK or offshore.

7.3 What are the risks associated with how long data is retained and how they might be mitigated?

	Privacy Risk	Mitigation
10	Breaching the DPA and Human Rights Act through excessive (or indefinite) retention of personal or sensitive data	• Disclosure and barring processes operate within DBS Data Retention Policies • DBS only holds information it needs to carry out its statutory functions • DBS has defined its rationale for the retention of information • Ensuring the integrity of the information is maintained • Ensuring the information is only retained for as long as necessary in accordance with the law • Detailing retention periods where a statutory retention period does not exist • Ensuring information collected and held is done so proportionately in accordance with the Human Rights Act 1998 • Ensuring information is accurate, relevant, kept up to date and is held securely.
11	Police data received from the NPIA or Police Service being retained for too long	• The data file containing the NPIA information will be overwritten each month • An audit file will be retained for four years • Police control retention and or destruction of their data • Local Police Forces have their own retention policies and can update the DBS system by updating the

		PNC.
12	Data shared with the TA, GTCW and WA is retained by them for too long	The TA, GTCW and WA have developed and implemented their respective data retention policies in order to comply with their respective mandates
13	Former CRB and ISA retention schedules not being appropriate for DBS	The DB Programme is reviewing the impact on retention schedules with the formation of the DBS
14	Considering the retention of different categories of information and data	With numerous categories and sensitivities of information, there are necessarily several approaches to retention employed by the DBS. Some information is under the direct control of the DBS, such as Barred Lists and Disclosure Certificate Information, however some retention approaches are controlled by the originator, for example PNC Nominal Information and Local Police Force Information which is controlled by the NPIA and the Local Police Force in question.
15	That payment details are retained too long and risk being acquired by a third party	• Credit/Debit cards have a limited lifetime • Payment data will only be retained for as long as it is required depending on the type of subscription opted for by the customer

7.5 What are the privacy risks associated with internal sharing within the Home Office and how they might be mitigated?

7.5.1 Most new internal information sharing privacy risks have been identified and explored in section 7.1 above. The exception to this is that the Home Office has proposed to exploit the current POISE Shared Services for both Desktop and Hosting for the Disclosure and Barring ICT solution.

7.5.2 There is a recognised risk that implementing the DBS system on the POISE Shared Service platform introduces additional risk based on the size of the user community and the number of supplier organisations that have indirect access to the POISE environment.

7.5.3 This risk is mitigated through requiring all DBS staff to be appropriately security cleared, the DB Programme developing additional controls to ensure that information is secure on the POISE environment. The Security Working Group for the DB Programme is evaluating (in conjunction with National Accreditors for PNC, GSi and the Home Office) to understand additional controls required. Two options being investigated include:

- Separation between the DBS application "Window" and other POISE functions, to prevent copying information from the DBS application to an externally facing email address or web system.
- Enhanced protective monitoring, to enable detection of inappropriate transfer of information.

7.6 Given the external sharing, what are the privacy risks and how might they be mitigated?

7.6.1 The majority of the external privacy risks have been considered in section 7.1 above. However, in addition to them, the following privacy risks have been identified:

	Privacy Risk	Mitigation
16	The new BPO supplier, TCS, will be using offshore development and UK-based service management. This poses a risk to personal information being inappropriately accessed, transferred or used.	• No direct or indirect network connections will exist between the POISE environment and offshore sites. • Any networks managed by the BPO that connect to POISE will be "air-gapped" from other networks operated by the BPO, and will not have connections to the Internet. • The BPO network will be fully accredited to IL3, subject to government network "Code of Connections" and ISO/IEC 27001, 27001 (Information Security Standard Requirements and Code of Practice). • BPO staff will have access to a very limited set of information, and will not be able to copy multiple records to the BPO network. • Pitney Bowes will operate as a sub-contractor to TCS to carry out the scanning and "mailing" services. Pitney Bowes operate an IL3 scanning facility. Information will be transferred securely from Pitney Bowes scanning operation to the DBS ICT solution. • No personal data will be handled outside the accredited environment. Specifically, no personal information will be taken offshore or be accessible offshore. • Offshore testing will be carried out

		with dummy data. • For testing against a PNC data source, the NPIA have committed to provide access to a test environment which can be connected using ISDN links (i.e. not via the internet). • All Systems Administration / Database Administration activity would be carried out by HOIT Shared Service staff in the UK (or equivalent, depending on the hosting solution deployed). These staff will all be "Police Vetted" – equivalent to SC vetting with additional Criminal Record and barring list checks.
17	Personal information may be lost or inappropriately used within the BPO contract.	• All BPO staff to be based in the UK • BPO staff will have access to only a small subset of incoming information; the full database of information is not available. • The network used for BPO operations network will not be connected to the internet, and will not be connected to other networks operated by TCS. • BPO users will have terminal appliance access to the ICT solution – this limits the functionality on POISE, preventing users having access to POISE functions such as email. This prevents data being transferred from the BPO network to other locations on the internet. • BPO network will be connected to the DBS via the GSi, ensuring conformance with the GSi "Code of Connection". • BPO service administration information will only be available to BPO users based in the UK. • Certificate details are sent from the BPO to the "secure printers" in encrypted form.
18	That an individual's payment details could be disclosed resulting	• Capita Payment Services have a

	in financial loss through the use of a third party payment provider	commercial contract with Capita that stipulates level 1 PCI DSS compliance. • Capita have confirmed that all procedures are in place to ensure that the payment system is PCI DSS compliant

7.7 How could risks associated with individuals being unaware of the collection be mitigated?

7.7.1 There is no new collection of data for the DBS to that previously undertaken by the CRB & ISA so no new risks in this regard have been identified.

7.7.2 To mitigate the existing risk to individuals being unaware of the collection of personal data, the following processes have been established for a considerable period of time:

- Disclosure service: Individuals complete the Disclosure application form and give their consent to the check being undertaken.

- Barring Service: On receipt of a referral, the Barring Service informs the individual concerned that a referral has been received and is being considered.

7.8 What are the privacy risks associated with redress and how might they be mitigated?

7.8.1 No privacy risks in relation to redress have been identified.

7.8.2 There are existing avenues of redress for both the Disclosure and Barring arms of the service. In terms of the Disclosure Service redress can be split into two groups:

- The customer believes that the information on the Disclosure Certificate does not relate to them, or elements of it are incorrect or irrelevant. There are two types of disputes – date entry and data source; a dispute process is in place for both types.
- The customer is unhappy with the service they have received from the Disclosure Service. In these circumstances, customers can complain to the DBS Customer Services.

7.8.3 For redress against the Barring Service, this would be against inclusion in one or both of the DBS Barred Lists for which there is an Appeal, Review and Complaints Procedure in place.

7.8.4 In the event of data loss, an individual would be able to seek redress through the Information Commissioner's Office.

7.9 Given access and security controls, what privacy risks were identified and how might they be mitigated?

7.9.1 The previous Access and Security controls within CRB & ISA have transferred to the DBS and are both sufficient and appropriate for access to data. Similarly, the Access and Security controls within the NPIA, TA, GTCW and WA are sufficient for the purposes of DBS. No further risks have been identified in this regard.

7.9.2 Additionally, access to paper documentation will be limited and considerably reduced compared to existing processes:

- Paper application forms and mail will be scanned and disposed of securely.
- The new DBS system will move towards case files becoming electronic rather than paper based, increasing the security and level of access controls available for information.

7.9.3 Access to ICT systems will only be possible using individual usernames and passwords. The POISE network is accredited for Impact Level 3. POISE desktops have no access to CD writers or memory sticks. POISE laptops have encrypted disks and RAS tokens for access when outside the Home Office estate. All DBS employees have achieved Level 1 of the National School of Government's e-learning course on Information Assurance. BPO staff members are provided with a lower level of access to disclosure and barring information.

7.9.4 In addition, the Programme has a SIRO and a number of IAOs. Their role is to understand what information is held, what is added and what is removed, how information is moved, and who has access and why. As a result they are able to understand and address risks to the information and ensure it is fully used within the law for the public good, and provide written input to the senior information risk owners (SIROs) annually on the security and use of their assets. These members of staff are also trained in Information Assurance to Level 3.

7.9.5 A full security accreditation process is planned and this will identify any additional controls required for highly sensitive information.

8. Overview

8.1 A change has been made to make the 'sensitive' flag visible to all users to enable them to easily identify sensitive cases and redirect any queries to the specialist DBS team.

8.2 A new requirement for the Update Service 'day 2' solution has been submitted that will limit access to sensitive cases to specified users.

8.3 A new requirement for the Update Service 'day 2' solution has been submitted that will only allow specified users to issue a so called '28 day reprint' of a Disclosure Certificate to RBs/Employers.

8.4 Scheduled Security Accreditation work will identify any additional controls required for sensitive information. The Programme Risk Register identifies security accreditation as a possible risk area (Risk 53):

*"**Security Accreditation of New IT System** - Lack of clarity between the bidder and HOIT about the security controls offered by the existing Shared Services Platform (SSP), may result in end-to-end security gaps in the new IT solutions so that there is a failure to achieve accreditation due to an unacceptable level of residual risk, leading to extra costs, failure to meet the deadline for go live and reputational damage.*

***Mitigating Action -** It has been agreed that the Programme is responsible for the end to end Accreditation strategy required to support the new DBS systems – within the Transition Workstream this will fall within the Business Design Authority Remit."*

8.5 The Programme recognises the importance of delivering appropriate security accreditation for the ICT solution and has an action plan in place. The supporting 'Off-shoring' PIA will be reviewed in early 2013, when the detail of accreditation requirements is understood.

8.6 The Transition PIA (one of those supporting this overall DBP PIA) will be developed in early 2013 and complete by Spring 2013. Once complete, this document will require updating and will need to be re-visited. Once updated, it should be re-considered by the Programme Board (or equivalent) for approval.

Document Author Signature

_____ Date: _____

Name (in capitals) _____

Approval Signatures (SRO/SIRO/IAO/HoI)

_____ Date: _____

Name (in capitals) _____

_____ Date: _____

Name (in capitals) _____

Acronym	Meaning
BPO	Business Process Outsourcing
BPSS	Baseline Personnel Security Standard
CRB	Criminal Records Bureau
CRM	Customer Relationship Management
CRR	Criminal Records Regime
CRSC	Criminal Record Status Check
DBP	Disclosure and Barring Programme
DBS	Disclosure and Barring Service
DPA	Data Protection Act
ECHR	European Convention on Human Rights
GIB	Group Investment Board
GRA	Gender Recognition Act
GRS	Gender Reassignment Surgery
GSI	Government Secure Intranet
HO	Home Office
HOIT	Home Office IT
HRA	Human Rights Act
HTTPS	Hypertext Transfer Protocol Secure
IAO	Information Asset Owner
ICO	Information Commissioner's Office
ISA	Independent Safeguarding Authority
NPIA	National Policing Improvement Agency
PCI DSS	Payment Card Industry Data Security Standard
PIA	Privacy Impact Assessment
PNC	Police National Computer
PNCID	Police National Computer ID
POFA	Protection of Freedoms Act 2012
RAS	Remote Access Service
RB	Registered Body
SIRO	Senior Information Risk Owner
SPPU	Safeguarding and Public Protection Unit, Home Office
SVGA	Safeguarding Vulnerable Groups Act 2006
VBS	Vetting and Barring Scheme
XML	Extensible Markup Language