Summary: Intervention & Options

Department /Agency:	Title:	
Ministry of Justice	**Impact Assessment of Enhancing the Commissioner's Inspection Powers with the Data Protection Act 1998.**	
Stage: Partial	**Version:** 01	**Date:** January 2009

Related Publications: Consultation Paper and Government Response on the Information Commissioner's Inspection Powers and Funding Arrangements under the Data Protection Act 1998 **http://www.justice.gov.uk/publications/cp1508.htm**

Available to view or download at:

http://www.justice.gov.uk/publications/coroners-justice-bill.htm

Contact for enquiries: Kavita Goburdhun **Telephone:** 020 3334 3809

What is the problem under consideration? Why is government intervention necessary?

The Information Commissioner's powers to conduct inspections and assessments under the Data Protection Act 1998 (DPA) are important mechanisms for regulating compliance with the data protection principles. However, Government sees benefit in enhancing his powers of inspection and investigation to improve the ability of the Commissioner to encourage and enforce compliance with DPA. This in turn will reduce the likelihood of data losses.

What are the policy objectives and the intended effects?

Effective and secure data sharing amongst organisations delivers improved public and private services, however reported high profile data breaches have reduced public confidence in this agenda. The policy objective of this proposal is to enhance the Information Commissioner's powers whilst undertaking inspections of compliance with the DPA. This will have the intended effect of identifying and rectifying problems before they escalate, and promote good practice.

What policy options have been considered? Please justify any preferred option.

(1) Retain the status quo; (2) Consider unfettered power of entry to inspect data controllers' systems; (3) Promote good practice and encourage data controllers to come forward for advice and (4) Enforce compliance and enhance the inspection powers of the Information Commissioner. We consider options (3) and (4) to have the most effective impact on encouraging compliance with the DPA.

When will the policy be reviewed to establish the actual costs and benefits and the achievement of the desired effects?

The Policy will be reviewed two - three years after implementation.

Ministerial Sign-off For final proposal/implementation stage Impact Assessments:

I have read the Impact Assessment and I am satisfied that, given the available evidence, it represents a reasonable view of the likely costs, benefits and impact of the leading options.

Signed by the responsible Minister:

Rt Hon Michael Wills MP, Minister of State at the Ministry of Justice

.....Date: 12 January 2009

Summary: Analysis & Evidence

Policy Option: 3 & 4	Description: **Promoting good practice and encouraging data controllers to come forward for advice** **Enforcing compliance and enhancing the inspection powers of the Information Commissioner**

COSTS

ANNUAL COSTS	
One-off (Transition)	**Yrs**
£ 2,500,000	1
Average Annual Cost (excluding one-off)	
£ 6,000,000	

Description and scale of **key monetised costs** by 'main affected groups'

The costs incurred by the ICO as a result of additional work will be met by a new funding structure (see consultation document . http://www.justice.gov.uk/docs/cp1508.pdf) Minimal costs will be incurred by the courts from an increase in the application for Schedule 9 warrants.

Total Cost (PV) **£**

Other **key non-monetised costs** by 'main affected groups' The costs noted above are not in addition to those noted in the impact assessment on ICO funding (see consultation document). Additional funds raised by the proposal on ICO funding are required to cover the cost of the functions covered in this impact assessment.

BENEFITS

ANNUAL BENEFITS	
One-off	**Yrs**
£ Nil	
£ Nil	

Description and scale of **key monetised benefits** by 'main affected groups'

Total Benefit (PV) **£**

Other **key non-monetised benefits** by 'main affected groups' The main benefit of the proposals is greater compliance by data controllers, leading to fewer data security breaches and greater public confidence in the Government's policy of data sharing.

Key Assumptions/Sensitivities/Risks A key assumption is that this proposal will ensure that the Commissioner has the appropriate range of tools required to carry out his responsibilities under the DPA, and that enhanced inspection powers will lead to a greater number of inspections carried out by the ICO.

Price Base Year	Time Period Years	**Net Benefit Range** (NPV) £	**NET BENEFIT** (NPV Best estimate) £

What is the geographic coverage of the policy/option?				United Kingdom	
On what date will the policy be implemented?				To be confirmed	
Which organisation(s) will enforce the policy?				ICO/Civil/Tribunal	
What is the total annual cost of enforcement for these organisations?				£ N/A	
Does enforcement comply with Hampton principles?				Yes	
Will implementation go beyond minimum EU requirements?				Yes	
What is the value of the proposed offsetting measure per year?				£ N/A	
What is the value of changes in greenhouse gas emissions?				£ N/A	
Will the proposal have a significant impact on competition?				No	
Annual cost (£-£) per organisation (excluding one-off)	Micro	Small	Medium	Large	
Are any of these organisations exempt?	No	No	N/A	N/A	

Impact on Admin Burdens Baseline (2005 Prices) (Increase - Decrease)

Increase £ Decrease £ **Net** £

Key: **Annual costs and benefits: Constant Prices** **(Net) Present Value**

Evidence Base (for summary sheets)

[Use this space (with a recommended maximum of 30 pages) to set out the evidence, analysis and detailed narrative from which you have generated your policy options or proposal. Ensure that the information is organised in such a way as to explain clearly the summary information on the preceding pages of this form.]

Proposal

The Data Protection Act 1998 (DPA) provides the Information Commissioner's Office (ICO) with an effective framework under which to regulate the DPA. Nevertheless, the Government recognises that it must continually develop this framework to ensure it keeps pace with advances in the technological and global climates.

The Government proposes to enhance the UK data protection framework by introducing a number of measures:

(1) **Promoting Good Practice**: Encouraging the uptake of good practice assessments by data controllers;

(2) **Enforcing Compliance**: Enhancing the Commissioner's Inspection Powers with the DPA;

(3) **Funding**: Amending the structure for the Information Commissioner's funding arrangements under the DPA.

This Impact Assessment concentrates on the first and second proposals; promoting good practice and encouraging data controllers to come forward for advice, and enforcing compliance by enhancing the Information Commissioner's inspection powers.

Part 1: Proposals

Government is putting forward two proposals to enhance the Commissioner's powers of external scrutiny. The first proposal is to encourage the uptake of good practice assessments by both data controllers and the Commissioner. This involves introducing an exemption from the civil monetary penalty under section 55A of the DPA (when it comes into force) for breaches discovered during a good practice assessment where a data controller has consented to the GPA.

The second proposal is to enhance the Commissioner's inspection powers. This involves:

- enhancing the Commissioner's powers under section 43 for the Commissioner to specify the time and place that any information should be provided under an Information Notice;

- strengthening the ICO powers under Schedule 9 to enable the Commissioner to require, during an on-site inspection, where a warrant is being executed, any person on the premises to provide the ICO with any information as appropriate to that investigation;

- providing the ICO with the power to conduct mandatory assessments of compliance of public authorities with the data protection principles

Policy Objectives and the intended effects

The policy objectives of these proposals are to ensure the Information Commissioner has sufficient powers to undertake inspections of data controllers, and to ensure compliance with the data protection principles. Increased external scrutiny provides a strong incentive for data controllers' to comply with their obligations under DPA. Ensuring that data controllers take

responsibility for the protection and safety of the data they hold will also serve to strengthen public confidence in the data protection framework.

Rationale for Change and Reason for Government Intervention

Encouraging Good Practice Assessments

The Information Commissioner has the ability to conduct Good Practice Assessments (GPA) under section 51(7) of the DPA. The GPA is intended as a co-operative process, whereby the Commissioner can work with data controllers to improve standards of compliance and provide advice.

The Commissioner may undertake a GPA with the consent of the data controller. This may include, for example, a data controller requesting an assessment or the Commissioner selecting an organisation in a high-risk area where processing involves sensitive data, and requests consent for a GPA. Encouraging good practice assessments will make data controllers aware of their responsibilities under the DPA. It will provide an opportunity for the ICO to work with data controllers to increase their understanding of their data protection responsibilities.

Government is aware that data controllers may be reluctant to request a GPA if they believe they could be penalised with a civil monetary penalty should a breach be discovered during the process.

Therefore, Government proposes to legislate to exempt a data controller who has consented to a GPA from the new civil penalty should a breach of the DPA be found in the course of that assessment. The ICO will, however, retain the power to use existing powers to issue Enforcement and Information Notices and powers to undertake prosecutions. This measure is designed to promote good practice, allowing data controllers to invite scrutiny, safe in the knowledge that no financial penalty would be imposed for problems identified.

Enhancing the Commissioner's powers of entry and inspection

Amendment to Section 43 of the DPA

Under Section 43 of the DPA, following a request from a data subject, or where the Commissioner reasonably requires information for the purpose of determining compliance with the data protection principles, the Information Commissioner can issue a data controller with an Information Notice. An Information Notice can require a data controller to provide the Commissioner with specified information, in a specified form, to assess a compliance with the data protection principles. Failure to comply with an Information Notice is a criminal offence under the DPA.

The Information Notice gives the Commissioner a power to inspect a data controller's compliance with the data protection principles. This provision empowers the Commissioner to specify the form in which information should be provided, giving substantial scope for its application. The Information Notice does not necessarily allow the Commissioner to go into a data controller's premises to carry out an inspection, but the Commissioner can require a specific document, or an explanation of a data controller's data protection policy and how it is used. The Commissioner could also follow up any request by issuing a further notice requiring an explanation of the information provided.

Government intervention is required to provide the Commissioner with greater powers to gather information to assess compliance. He may wish to use his powers if he feels that a data controller is attempting to avoid providing information he needs to carry out his duties. While the Commissioner can set a deadline by which information should be provided under section 43, there is no explicit power to specify the time and place that information should be provided to the Commissioner.

We propose to enhance the powers under section 43 to be able to specify the time and place that any information should be provided to the Commissioner. This may also prove useful where the information that the Commissioner requires can not be easily or securely sent to the ICO, or if the Commissioner needs the data controller to provide the information quickly and in person. In practice, this would allow the Commissioner to serve an Information Notice on a data controller, for example, requesting them to provide an explanation of their data security procedure at 10:00am at the data controller's premises. Similarly the Commissioner could require the data controller to attend the Commissioner premises to provide the requested information.

Increasing powers under Schedule 9 warrant
Inspections can provide a strong deterrent to non-compliance, and can be a proactive way to identify and rectify problems before they have a chance to escalate.

The Commissioner has the explicit power to undertake an on-site inspection or assessment in certain circumstances. These circumstances are:

- when a data controller consents to an assessment by the Commissioner for good practice;

- when the Commissioner has reasonable grounds for suspecting the data protection principles are not being complied with and has obtained a search warrant from a judge to conduct an assessment; and

- to assess whether data held in certain international data systems is being processed in accordance with the DPA.

While obtaining consent for an inspection is preferred, in cases where this has not been obtained, and the Commissioner needs to carry out an inspection to determine whether the data controller has breached the DPA, he may wish to apply to the court to obtain a warrant to enable him to carry out his duties. This is a separate and more powerful tool than requesting or obtaining information by way of an Information Notice. Section 50 and Schedule 9 of the DPA provide the Commissioner with the power to apply to a judge for a warrant to enter and search premises (including inspection and examination of equipment and documents) without consent.

Currently the DPA does not provide the Commissioner with explicit powers to request an explanation of any information he finds during an on-site inspection or investigation. Reviewing documents or testing systems may sometimes provide only part of the picture, and could limit the Commissioner's ability to understand the true nature of data processing within an organisation.

To overcome these issues, Government proposes to extend the Commissioner's powers under Schedule 9. This will allow him to require any person on the premises where a warrant is being executed to provide him with any information he reasonably requires for the purpose of determining whether the data controller has complied with or is complying with the data

protection principles. This would allow the Commissioner to request information in the form of an explanation.

Government also proposes that the Commissioner should be able to apply to the court for a warrant on the basis of a risk assessment. Completing the risk assessment would help to identify data controllers who were unlikely to be complying with standards but also those engaged in high-risk processing.

A table of the number of warrants that have been applied for by the Information Commissioner over the last few years is at Annex A. It is not expected that this proposed enhanced power will lead to an increase in the number of warrants being issued by the courts, and in most cases the Commissioner will continue to obtain access to information or premises working in co-operation with data controllers.

Conducting mandatory assessments of the compliance of public authorities with the data protection principles

Following the loss of child benefit data by HMRC on 21 November 2007, the Prime Minister made a statement that the Information Commissioner would be entitled to carry out "spot checks" for DPA compliance on all Government Departments. In the wake of this announcement the powers in section 51(7) of the DPA were identified as being an appropriate basis for such checks (an assessment under section 51(7) is often referred to as a good practice assessment). This proposal does not require legislation.

However, Government sees a vital distinction between public and private authorities in the handling of personal data. Government does not want to impose further burden on business, but more important is the nature of the information that public authorities hold and process, and the fact that the handling of this data is necessary to most individuals. It is difficult for any person to live their life without disclosing and having personal information processed by a variety of public bodies. It is therefore important to the rights of individuals, and to their confidence in public authorities, that their personal data is safeguarded.

Government therefore proposes to give the Information Commissioner power to assess a public authority for compliance with the Data Protection Principles. It is envisaged that the assessment will be conducted in two stages. The first stage will involve the Information Commissioner reviewing the policies and procedures of the Public Authority. The second stage will be a compliance assessment (which may involve an on-site inspection), which will look at specific cases and verify that these policies and procedures are being put into practice. This process will be very similar to standard audit practice and the agreed arrangements for the "spot checks" of Central Government Departments.

The key objective with this policy is to strike a balance between the powers of the Information Commissioner and the need for the business of Government and the wider public sector to continue unhindered. Although an assessment of a public authority will be conducted without consent it is not the intention that the Information Commissioner will, for example, be conducting extensive searches of premises. These assessments will be more collaborative and aimed at assessing compliance.

Proposed amendments to the Data Protection Act

Some of these proposals would require amendments to the DPA, specifically:

- amendment to facilitate an exemption from the civil monetary penalty under section 55A of the DPA (when it comes into force) for breaches discovered in the process of a GPA where a data controller has provided prior consent to a GPA;

- amendment to section 43 to include ability to specify time and place that any information should be provided to the Commissioner in an Information Notice;

- amendment to Schedule 9 to allow the Commissioner to require an explanation of any information found on the premises;

- amendments to Schedule 9 of the DPA to allow the Commissioner to apply for a warrant in cases where he does not have reasonable grounds to suspect a breach of the data protection principles, whether or not a risk assessment has been undertaken:

- amendment to the DPA to create a new proposal to allow the Information Commissioner to conduct mandatory assessments of compliance of public authorities with the data protection principles.

Part II Policy options that have been considered.

(1) Retain the status quo;

(2) Consider unfettered power of entry;

(3) Encourage the use of good practice assessments; and

(4) Amend current legislation to enhance the inspection powers of the Information Commissioner.

We consider, taken together, the proposals under option (3) and (4) will have the most effective impact in ensuring data controllers are fully with the DPA, reducing the likelihood and severity of any future data protection breaches.

Pros, cons and risks of each option

Option 1 – Retain the status quo

The benefit of retaining the status quo is that no new costs would be incurred. However, not doing anything means that there is limited incentive for data controllers to ensure compliance with the DPA. Doing nothing also limits the effectiveness with which the Information Commissioner can conduct inspections.

Option 2 – Consider unfettered power of entry

While a limited number of other regulators have the power to enter premises at any time for the purpose of carrying out their regulatory duties, this generally predates the Human Rights Act 1998 (HRA). The HRA implements Article 8 of the ECHR, which provides a right to respect for private and family life, home and correspondence. For example, the Health and Safety Act 1974 gives local government authorities the power to enter premises at any time for the purpose of carrying into effect any of the relevant statutory provisions; the Competition Act 1988, the Consumer Credit Act 1974, and the Enterprise Act 2002 gives the Office of Fair Trading the power to obtain entry without a warrant in certain circumstances.

The benefits of giving the Information Commissioner an unfettered power of entry is that he will have ultimate powers of entry to inspect the premises of data controllers who he suspects have committed, are committing, or are likely to commit, a breach of the data protection principles. Organisations who are knowingly in breach of the data protection principles would not be able to evade inspection of their data systems and would risk being subject to appropriate enforcement action.

This option carries a significant risk of alienating data controllers rather than encouraging them to work with the Commissioner. Not pursuing this option also carries a risk of data controllers evading investigation by the Commissioner, however we propose to mitigate this risk through other options.

Given the importance of the Commissioner's role to educate and promote good practice, and his preference for a co-operative regulatory environment, we consider the option for unfettered power of entry to premises too extreme.

Option 3 – Encourage the use of good practice assessments

This option provides a more efficient way to gain consent for a good practice assessment, and in turn, facilitates the assessment process. This option encourages data controllers to participate in a GPA, which provides an effective vehicle for education and compliance through co-operation. Data controllers would benefit from targeted guidance from the Commissioner, increasing the standards of data protection.

We do not believe that there are disadvantages to this proposal. One risk of this proposal is that some data controllers who do not provide consent for a good practice assessment may not participate in this process, missing the opportunity to improve their data management systems. This risk exists in the current regulatory environment and is mitigated by the Commissioner's powers to formally investigate compliance with the DPA.

Providing an exemption from the civil monetary penalty under section 55A of the DPA (when it comes into force) for breaches discovered in the process of a GPA, where a data controller has provided prior consent to a GPA, will encourage data controllers who wish to handle data appropriately but are not sure of their regulatory obligations to come forward for advice. This will result in higher compliance levels and foster good practice.

Option 4 – Enhance the inspection powers of the Information Commissioner

The benefit of this option is that these proposed amendments to the DPA are complimentary to the Commissioner's existing powers, and provide clarity for data controllers and the Commissioner about the extent of information that can be requested throughout an investigation. The proposals to enhance the Commissioner's powers under Schedule 9 will ensure that the Commissioner has access to relevant information in order to carry out his duties and to gain a more accurate understanding of an organisation's compliance with the data protection principles.

The extension of carrying out assessments across the public sector, without consent, will have the effect of ensuring data controllers are compliant with the DPA, especially if they may be liable to a financial penalty.

This proposal carries a risk of negative feedback from non-compliant organisations, however the Government considers that the Commissioner requires a range of enforcement tools, including the ability to take decisive and strong action where necessary in order to carry out his duties. This option would not affect data controllers who are co-operative and genuinely committed to meeting their regulatory requirements.

Main affected groups

The main group affected by our proposals is data controllers in the UK, including public and private sector organisations. In April 2008, there were 304,551 registered data controllers in the UK.

Analysis of Costs and Benefits

Option 1

This would is cost neutral. No additional costs or benefits would be generated.

Option 2

This option would ensure the Commissioner has easy access to premises of data controllers in order to carry out his duties and provide a powerful incentive to data controllers to comply with their regulatory obligations under the threat of an inspection.

Assuming that this option would only be employed in extraordinary circumstances, there would be minimal costs involved in implementing this proposal. If it were to be used for other purposes, such as random checks of compliance, then costs could include additional resources for the ICO to carry out the inspections.

Government believes that giving the Information Commissioner an unfettered power of entry to inspect systems would not achieve our policy intentions for the following reasons. The Information Commissioner wants to emphasise a co-operative regulatory environment by promoting good practice through education. We also want to ensure that the Commissioner has appropriate powers to enforce compliance, however we consider that an unfettered power of entry would be a disproportionate way to achieve these policy intentions.

Option 3

The costs of this proposal would include additional resources for the ICO in carrying out a greater number of good practice assessments, and costs to data controllers of participating in the assessments. We propose that the ICO costs are met by the Government's proposal to address ICO funding.

Businesses are more likely to sign up to these assessments if the costs of doing so are less than the benefits. Whilst there will be additional costs on those organisations who are inspected, in terms of making data/staff available, we believe these costs will be far outweighed by the benefits of an inspection.

The benefits of encouraging good practice assessments are that data controllers will have increased access to advice and guidance from the ICO, relevant to their specific organisation. This would increase compliance and strengthen data security, reducing the likelihood of a breach occurring or the imposition of a fine (when section 55A of the DPA is enacted). This will, in turn, lead to greater customer satisfaction and a safer environment for data sharing.

Option 4

Enhancing the inspection powers of the Information Commissioner will ensure that the Commissioner has access to the information he requires to effectively carry out his duties, particularly where the Commissioner suspects a data controller is trying to evade investigation.

This option would incur costs to the ICO of making inspections and to companies receiving the inspections. We are looking into the funding arrangements of the Information Commissioner's Office for his increased data protection work and this option has been factored into those proposals.

There will be some costs for data controllers associated with compliance of Section 43 of the DPA in ensuring that the relevant information is provided to the Information Commissioner, however the only new aspect of this proposal is for a specific date and time for compliance. A route of appeal against an Information Notice currently lies direct to the Information Tribunal. However, data controllers will have the opportunity to go back to the Information Commissioner and ask him to reconsider the deadline. We expect this will reduce the number of any eventual appeals to the Information Tribunal.

The new proposal under Schedule 9 will also have minimal impact for data controllers in terms of providing assistance to the Information Commissioner, as will those public authorities who may be subject to a compulsory assessment. There may be an increase in the number of applications for warrants, however we do not expect this increase to be significant as we do not anticipate a sharp increase in the number of circumstances where the Commissioner would need to escalate his actions to this level. The costs to the judicial system are therefore anticipated to be minimal.

It is estimated that, once the ICO's office is fully resourced to its full complement, there will be approximately 105 assessments conducted every year on public authorities and private companies. This figure is based upon current resources involved in an assessment, which will allow for approximately 17 inspections to be carried out a year. It is intended to create five inspection groups, with the possibility of a further 20 assessments being outsourced - these costs will be met from the new fee regime. The breakdown of these assessments is currently not clear, and will be driven to a large extent by the identification of risks.

The ICO will produce a Code of Practice setting out the standards at which they will operate while carrying out these assessments. This will ensure that the ICO is acting fairly and reasonably while carrying out these assessments, which will reduce the number of potential appeals to the Information Tribunal.

We anticipate that these proposals, in time, will bring about a change in behaviour towards data security for data controllers, increasing compliance and reducing the need for inspections.

Benefits to this proposal includes greater customer satisfaction, lower levels of fraud and more confident consumers.

Options Conclusion
Given the identified need to address the limitations of the existing data protection framework the Government does not consider it appropriate to do nothing (option 1). We also do not consider that giving the Information Commissioner unfettered access to data controllers' premises (option 2) is an appropriate or proportionate way to achieve improvements in compliance with the data protection principles.

The Government considers that a mix of encouraging good practice (option 3) and enhancing the Commissioner's inspection powers (option 4) will address the needs of the existing framework and help build confidence in the strength of the data protection framework.

Administrative burdens and simplification
Options 1 would not have any additional administrative burdens. Option 2 would incur a burden on data controllers, as they would need to resource the Commissioner's inspection without notice and with little time to arrange cover. An unannounced inspection would disrupt daily business operations. Option 3 implies a small administrative burden for data controllers whereby they will be asked to provide prior consent to a good practice assessment when they register as a data controller with the ICO. We envisage this burden to be minimal. There are also small administrative burdens for data controllers in general relating to option 4. For those organisations to which option 4 applies, we consider the burden of providing relevant information about their compliance, as well as participating in assessments as appropriate and proportionate to enable the Commissioner to carry out his duties effectively.

Enforcement, sanctions and monitoring
Options (1), (2) (3) or (4) will not have any impact on enforcement.

Competition Assessment
No measurable competition impact is foreseen.

Small Firms Impact Test
Options (1), (2), (3) and (4) have no greater impact on small firms as present.

Legal Aid/Judicial Impact
Options (1), (2), (3) and (4) has little additional impact on legal aid or on the judiciary.

Equality Assessment & Human Rights

These proposals concern data controllers. None of the options considered have any impact on Race, Disability or Gender of individuals. They are compliant with the Human Rights Act.

Public Authorities

Options (1) and (2) would not have any additional impact on public authorities, although there will be an impact on public authorities if they obstructed the Information Commissioner from inspecting their systems and he had a power of entry without a warrant. However, we do not believe that public authorities will be uncooperative with the Information Commissioner. Option (3) or (4) will not have an impact upon Public Authorities unless their systems are being inspected.

Specific Impact Tests: Checklist

Use the table below to demonstrate how broadly you have considered the potential impacts of your policy options.

Ensure that the results of any tests that impact on the cost-benefit analysis are contained within the main evidence base; other results may be annexed.

Type of testing undertaken	*Results in Evidence Base?*	*Results annexed?*
Competition Assessment	Yes	No
Small Firms Impact Test	Yes	No
Legal Aid	Yes	No
Sustainable Development	No	No
Carbon Assessment	No	No
Other Environment	No	No
Health Impact Assessment	No	No
Race Equality	Yes	No
Disability Equality	Yes	No
Gender Equality	Yes	No
Human Rights	Yes	No
Rural Proofing	No	No

Annexes

Annex A

Number of warrants applied for by the Information Commissioner, 2005/06-2006/07

Year	No of warrants applied for	% of cases opened
2006/07	7	0.03
2005/06	12	0.05