

The Framework for the Provision of Employment Related Support Services

Security Plan and Guidance for Completion

August 2010

Tender round title:	The Framework for the Provision of Employment Related Support Services	
Organisation name:	<i>Insert Your Organisation Name</i>	_SEC

PROTECT – COMMERCIAL

Department for Work and Pensions – The Framework – Invitation to Tender

Important Information

This form is designed to provide you with the guidance and information requirements needed to complete a Security Plan as required by The Framework for the Provision of Employment Related Support Services and subsequent (DWP) contracts called off under the Framework Agreement

Before completing the form you are advised to read the following documents carefully along with the covering letter:

- The Framework Invitation to Tender (ItT) Instructions for Bidders;
- Provider Guidance pages on the Welfare to Work section of the Supplying DWP website;
- The Specification of the Commercial Requirement for The Framework
- The DWP Framework Terms and Conditions applicable to this contract and subsequent call-off Terms and Conditions (will form Schedule 4 of Framework Terms and Conditions) - *these may be subject to change before contract award.*

Introduction

The spreadsheet embedded in Section 3 provides an outline Security Plan that sets out the security measures to be implemented and maintained by Providers in relation to all aspects of the services and all processes associated with the delivery of Provider Referral and Payment (PRaP) as required by the Framework Terms and Conditions (T&Cs): Schedule 9 - Security Requirements & Plan.

Schedule 9, Section 2 requires Providers to be responsible for the security of the Prime Contractor System (which in the context of the Security Plan is defined as “PRaP Provider Information Systems and Services”) and requires that they shall at all times provide a level of security which:

- a) is in accordance with Good Industry Practice and Law
- b) complies with DWP’s Security Policy (“ISSS”)
- c) complies with ISO/IEC 27002 and ISO/IEC 27001 (“ISO 27001”) ¹
- d) meets specific security threats to the Contractor System

The embedded “Outline Provider Security Plan” is structured in accordance with the international standard for Information Security Management ISO 27001 and links together references relating to a), b) and c) above. This is intended to aid Providers in producing a Security Plan that addresses all contractual security requirements.

¹ It should be noted that in DWP’s Framework T&Cs: Schedule 9, the requirement for the Provider to obtain independent **certification** to ISO 27001 has not been specified. However the Provider is required to **comply** with the principles and practices of ISO 27001.

PROTECT – COMMERCIAL

Department for Work and Pensions – The Framework – Invitation to Tender

DWP recognise that Providers will likely have their own different implementations of PRaP Provider Information Systems and Services. In order to determine the specific security threats as per d) above, it is necessary for each Provider to provide the following details in Section 1, 2 & 3 below to allow the scope of their Security Plan to be assessed by DWP.

NB Following acceptance on to the Framework , and as an enduring obligation throughout the term of the Framework, the Prime Contractor shall develop and maintain (in conjunction with the Authority but, for the avoidance of doubt, at the Prime Contractor's own cost and expense) the draft Security Plan, which will form Appendix B of Schedule 9 of the Framework Ts and Cs.

In respect of each Call-Off Contract which may be entered into with the Authority or any Other Contracting Body, the Prime Contractor shall, at all times, comply with the security requirements set out in the Order Form and/or the Call-Off Terms and Conditions (Schedule 4) or such other security requirements as notified by the Authority (or the relevant Other Contracting Body, as the case may be) to the Prime Contractor from time to time.

Overview

Basic Information

Providers are required to scope the information systems in the context of the organisation's business in relation to PRaP Provider Information Systems and Services. It must describe the security-relevant aspects of the system in order for the specific security threats to the PRaP Provider Information Systems and Services to be determined.

How to submit the information required

You should embed your responses for each part of Section 1 as a composite response placed below Section 1.3; i.e. to include answers to section 1.1, 1.2 and 1.3.

Response to Section 2 should be embedded below the section.

Provide your proposals for offshoring data in the space provided at section 3

You should complete the Outline Provider Security Plan embedded at Section 3, save and close using an Excel version compatible with 2000 version.

Definitions of Terms are contained within Section 4.

This entire document must then be submitted as described in the Instructions for Bidders, using Microsoft Word and, or Excel compatible with 2000 version.

PROTECT – COMMERCIAL

Department for Work and Pensions – The Framework – Invitation to Tender

1 Solution Overview

1.1 Business Context of PRaP Provider Information Systems and Services

This shows that the business needs of the organisation are understood and fed into the risk management process, and your answer should cover:

- Organisational ownership of the Asset
- High level business aims and objectives served by the Asset
- Business functions supported by the Asset
- Information processes carried out by the Asset

Data flow and / or process diagrams may be useful.

1.2 Description of the Information Systems and associated Assets of PRaP Provider Information Systems and Services

Your response should provide a pen picture of:

- Information assets (description, quantity, sensitivity)
- Software (main items, with reference to inventory)
- Physical Assets (computer equipment and buildings)
- Services (network services, heating, lighting, power, air-conditioning)
- People (user numbers, roles, groups, organisations, security clearances)

All significant Assets should be recorded by the Provider in an Asset Inventory.

Schematic architecture diagrams should be provided.

Where subcontractors and / or 3rd Parties are used, and they have access to PRaP Provider Information or PRaP Provider Information Systems and Services, the following details should be provided for each organisation:

- Name of subcontractor / 3rd Party
- Service they provided to Prime Contractor
- Access to which PRaP Provider Information data fields
- Number of staff with access to the above DWP data
- Locations of staff with access to the above DWP data

PROTECT – COMMERCIAL

Department for Work and Pensions – The Framework – Invitation to Tender

- Access method to PRaP Provider Information or PRaP Provider Information Systems and Services

A spreadsheet template is embedded below if you wish to use it to capture the above data.



Subcontractor
Questionnaire

1.3 Interconnections, Interfaces, Shared Infrastructures & Related Security Domains of PRaP Provider Information Systems and Services

- Document and describe each external connection

- Document and describe any shared infrastructures (networks and systems) that are used and how they relate to non PRaP specific services

Details may include ownership, business need, data flows, technical details, sensitivities and the security status of the any connecting or shared systems.

Diagrams should be provided to illustrate the above.

2 Security Threats

Provide details of the perceived security threats to PRaP Provider Information Systems and Services and document security counter-measures implemented to address each security threat.

A table may be useful to illustrate the above that relates to controls within the Security Plan.

3 Security Plan

The Department's data containing personal information must be handled in accordance with the data protection legislation in force within the UK and must not, under any circumstance, be offshored. The requirement below refers to non personal data.

The Department's non personal data must not be processed outside the United Kingdom without the prior written consent of DWP and must at all times comply with the Data protection Act 1998.

PRaP Provider Information must not be processed outside the United Kingdom without the prior written consent of DWP and must at all times comply with the Data Protection Act 1998 and any other relevant data protection legislation.

PROTECT – COMMERCIAL

Department for Work and Pensions – The Framework – Invitation to Tender

If your solution has an element of offshoring you will be required to complete the DWP's Offshoring Form, which will be reviewed by the DWP's Security, Offshoring and Legal teams. A significant level of detail around the proposed solution will be required, and it is likely that the offshoring of any personal data will not be authorised due to risk to the data.

Please confirm in the space below whether you are considering or intending to offshore any PRaP Provider Information as part of your delivery proposal and if so please explain how non-agreement of such proposals would affect your position in this competition.

Are considering or intending to offshore any PRaP Provider Information	Yes	No

Complete the details in the attached Outline Provider Security Plan for the PRaP Provider Information Systems and Services to be utilised in the delivery of this contract.



Outline Provider
Security Plan

Further guidance for completion of this is shown in the Notes section of this spreadsheet.

4 Glossary of Terms

The following provide relevant extracts from DWP documents that are intended to provide guidance in the interpretation of the Security Plan requirements and terms.

Relevant Terms as Referenced in the DWP FND Ts&Cs

The contract is between **DWP ('The Authority')** and **Provider ("Prime Contractor")**

Terms within Contract Interpretation and Schedule 9

Authority Data means

- a) the data, text, drawings, diagrams, images or sounds (together with any database made up of any of these) which are embodied in any electronic,

PROTECT – COMMERCIAL

Department for Work and Pensions – The Framework – Invitation to Tender

magnetic, optical or tangible media, and which are:

i) supplied to the Prime Contractor by or on behalf of the Authority; or

ii) which the Prime Contractor is required to generate, process, store or transmit pursuant to this Agreement; or

b) any Personal Data for which the Authority is the Data Controller.

Breach of Security	the occurrence of unauthorised access to or use of the Authority Premises, the Sites, the Services, the Prime Contractor System or any ICT or data (including the Authority's Data) used by the Authority or the Prime Contractor in connection with this Agreement.
Commercially Sensitive Information	means any Confidential Information comprised of information: a) which is provided by the Prime Contractor to the Authority in confidence and designated as Commercially Sensitive Information; and/or b) that constitutes a trade secret.
Confidential Information	means any information which has been designated as confidential by either Party in writing or that ought to be considered as confidential (however it is conveyed or on whatever media it is stored) including information which relates to the business, affairs, properties, assets, trading practices, Provision(s), goods and services, developments, trade secrets, Intellectual Property Rights, know-how, personnel, customers and suppliers of either party, all personal data and sensitive personal data within the meaning of the Data Protection Act 1998 and the Commercially Sensitive Information.
Data Controller	shall have the meaning given to it under the DPA.
DPA	means the Data Protection Act 1998 (as amended).
DWP Information Systems Security Standards (ISSS)	The Standards are based on and follow the same format as ISO/IEC 27001, but with specific reference to the DWP's use.
Personal Data	shall have the meaning given to it under the DPA.
Provision	means a Provision for the delivery of goods and services the details of which are more fully described in Schedule 2 (The Provision) to this Contract and the relevant Annex to that Schedule. For the avoidance of doubt, the Prime Contractor may be delivering one or more Provisions

PROTECT – COMMERCIAL

Department for Work and Pensions – The Framework – Invitation to Tender

under the terms of this Contract.

Security Plan

means the Prime Contractor's security plan prepared pursuant to Section 3 of Schedule 9 (Security Requirements and Plan).

Security Policy

means the Authority's Security Policy annexed to Schedule 9 (Security Requirements and Plan) as updated from time to time.

Security Tests

shall have the meaning set out in Paragraph 4.1 of Schedule 9 (Security Requirements and Plan).

Sensitive Personal Data

shall have the meaning given to it under the DPA.

Site

means any premises from where the Provision(s) is provided or from which the Prime Contractor manages, organises or otherwise directs the provision or the use of the Provision(s), including for the avoidance of doubt any such premises used by the Prime Contractor's agents or sub-contractors from time to time.

Terms within the Outline Provider Security Plan

Aggregation

There are two circumstances that can lead to aggregation:

Accumulation - the building up of small amounts of data into a large volume held in one place or transmitted electronically.

Association - the combination of different types of information which when combined have a higher impact, when compromised, than that of the individual type of information. The criteria under which aggregation applies will depend upon the type of information and the circumstances in which it is accessed, stored, processed or transmitted. Where information is aggregated the potential impact of compromising that information can be significantly higher than the potential impact of a compromise of a small amount of the underlying information. For instance the compromise of information relating to a single person is much less than the impact of compromising equivalent information relating to thousands or millions of people.

Asset

Assets associated with PRaP Provider Information Systems and Services include:

- a) information;
- b) software;

PROTECT – COMMERCIAL

Department for Work and Pensions – The Framework – Invitation to Tender

c) physical assets, such as computer equipment and buildings;

d) services, such as computing and communications services, heating, lighting, power and air-conditioning;

e) people.

BPSS

Baseline Personnel Security Standard.

FIPS

Federal Information Processing Standards (FIPS) that are developed by the US National Institute of Standards and Technology (NIST) for US Federal computer systems.

A number of these standards are recognised by UK HMG, including: FIPS 140-2 SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES.

ISO/IEC 27001 (ISO 27001)

Information Security Management Systems (Requirements).

ISO/IEC 27002 (ISO 27002)

Code of Practice for Information Security Management.

Offshoring

Hosting or accessing Authority Data from outside of the UK.

PRaP

Provider Referral and Payment.

PRaP Information Classification

Information that has been classified in terms of its value, legal requirements, sensitivity and criticality to the Provision.

Information classifications are designed to help individuals determine, and indicate to others, the levels of protection required to help prevent the compromise of valuable or sensitive assets. Applying a protective marking to an Asset indicates the level of protection required.

The definition for each level of information classification can be formulated to cover a wide range of documentary and other types of Assets, which include:

a) paper based documents;

b) information held and transmitted in electronic form;

c) microfilm;

d) valuables and cash;

e) IT equipment.

(Within Government this term is known as “protective marking” but Provider’s may have their own existing information classifications that can be applied as

PROTECT – COMMERCIAL

Department for Work and Pensions – The Framework – Invitation to Tender

appropriate).

PRaP Provider Information Systems and Services

Any information system or service that the Provider relies upon for the Provision that stores, processes or communicates PRaP Provider Information, even where the Provider does not own that system or service.

PRaP Provider Information

These are information Assets that include information obtained from DWP defined within DWP's FND T&Cs as "Authority Data" for the Provision that includes, but is not limited to:

- a) Personal Information - information the DWP holds about its customers and staff;
- b) business support information - information generated to support its business functions, such as policy, management and accounting information, internal telephone directories, circulars and staff codes and manuals;
- c) audit information - technical, transactional and business audit record;
- d) system documentation associated with the design, development, testing and operation of PRaP Provider Information Systems and Services.

Secure Area

Locations where there is a special security need such as those holding PRaP Provider Information or PRaP Provider Information Systems and Services of a sensitive nature or where the equipment may be critical to the operation of the system or service.

Security Incident

A single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

Additional definitions of general information security terms, which may be used in the Outline Provider Security Plan and elsewhere, are available in ISO/IEC 27000 – Information Security Management Systems (Overview and Vocabulary) which is available for free from the ISO website at:

http://standards.iso.org/ittf/PubliclyAvailableStandards/c041933_ISO_IEC_27000_2009.zip

PROTECT – COMMERCIAL

Department for Work and Pensions – The Framework – Invitation to Tender

Appendix – Security Plan Assessment and Approval

Purpose

For those organisations that have been chosen as Preferred Bidders or Prime Contractors, this additional information is designed to help with the Security Plan assessment process by highlighting some key areas that have to be addressed before approval can be given to receive DWP data and to connect to Provider Referral and Payments System (PRaP).

From experience, the delivery timescales on some contract packages has been ambitious and it was felt that by providing an early sight of the critical aspects of the Security Plan assessment process it would help planning the design, development, delivery and operational management of your PRaP Provider Information Systems and Services.

1 Security Plans

1.1 Incomplete Plans

As indicated in the guidance above, there are 3 Sections to the Security Plan:

1. Solution Overview
2. Security Threats
3. Security Plan (*spreadsheet*)

All of these sections **must** be completed before the Security Plan can be assessed and any approval given. Delays to the assessment process will be experienced if all sections are not completed and submitted in a timely manner, as they are all essential. If you need advice as to how to complete the plan please contact DWP as soon as possible.

1.2 Supporting Documentation

As part of the assessment process we will ask to see any documents (e.g. policies or procedures) referred to in the Security Plan, or necessary to evidence any claims. The process can be speeded up if copies of these are provided with your Security Plan submission.

The Security Assessors would expect to see a comprehensive set of information security policies, procedures and standards that support the security of the PRaP Provider Information Systems and Services, with a particular focus on all the controls related to confidentiality.

1.3 Early Submission

We need to get through the Security Plan assessment process in time for the go live date, so please submit your documentation as early as possible. We understand that the Security Plan is part of a whole raft of issues that need to be addressed but without an

PROTECT – COMMERCIAL

Department for Work and Pensions – The Framework – Invitation to Tender

approved Security Plan there is a risk that service commencement is impacted or delayed. We would ask that production of the Security Plan and addressing any related issues is given the appropriate priority.

1.4 Assessment Process

Stage 1 – Documentation Review

Stage 2 – Verbal & Written Q&A with Provider

Stage 3 – Pre-Assessment Site Visit

Stage 4 – Assessment Site Visit(s)

Stage 5 – Assessment Write-up and Scoring

Stage 6 – Penetration Testing and Reporting

Stage 7 – Agreement with Provider on Corrective & Remedial Actions

Stage 8 – Submission to DST and SRO for Approval

2 Offshoring Data

PRaP Provider Information must not be processed outside the United Kingdom without the prior written consent of DWP and must at all times comply with the Data Protection Act 1998 and any other relevant data protection legislation.

If your solution has an element of offshoring you will be required to complete the DWP's Offshoring Form, which will be reviewed by the DWP's Security, Offshoring and Legal teams. A significant level of detail around the proposed solution will be required, and it is likely that the offshoring of any personal data will not be authorised due to risk to the data.

Please confirm whether or not you are considering or intending to offshore any PRaP Provider Information as part of your delivery proposal and if so please explain how non-agreement of such proposals would affect your position in this competition.

Providing access to PRaP Provider Information, for example over a VPN connection, from non-UK locations may also be considered to be offshoring and the above points apply.

NB Early notification is essential as the approval process is lengthy and complex. Also, there is no guarantee of success and the Provider should have a contingency plan if the request is not approved, or is approved after go-live.

PROTECT – COMMERCIAL

Department for Work and Pensions – The Framework – Invitation to Tender

3 Personnel Security

DWP requires all individuals (Prime, subcontractors, and authorised 3rd Parties) who may have access to PRaP Provider Information to hold, at a minimum, a security clearance of Baseline Personnel Security Standard (BPSS). No access to the information is permitted without this clearance. Please see the following references for further details:

<http://dwp.gov.uk/docs/aguidefordwpcontractors.pdf>

http://www.cabinetoffice.gov.uk/spf/mandatory_requirements/mr23.aspx

The BPSS comprises verification of four main elements:

1. Identity
2. Employment History (3 years)
3. Nationality & Immigration Status (*including Right to Work*)
4. Unspent Criminal Records

You need to make sure that your recruitment processes take these requirements into account and that you allow enough time to undertake the necessary checks with Disclosure Scotland or Criminal Records Bureau (CRB). This requirement is equally necessary for existing staff and, if they meet the standard, HR records may be utilised.

From experience, some Providers have left it too late and have had insufficient cleared staff in place to handle business. Please consider clearance requirements in good time.

NB The above BPSS obligation does not replace any legal, regulatory or contractual requirements for a higher level of personnel security clearance or government vetting.

4 Encryption

DWP security authorities advise that the use of encryption technologies, validated to FIPS 140-2 as a minimum, should be deployed by Providers where PRaP Provider Information is in storage or in transit.

DWP expects to see Providers implementing encryption wherever Personal Data is stored (including laptops, desktops, servers, backup and removable media) or communicated (including over e-mail, web browser / terminal sessions, VPNs and database connections).

Details of FIPS 140-2, and which vendors and products have been validated, are contained on the National Institute of Standard and Technology (NIST) website:

<http://csrc.nist.gov/groups/STM/> (overview)

<http://csrc.nist.gov/groups/STM/cmvp/validation.html> (validation lists)

PROTECT – COMMERCIAL

Department for Work and Pensions – The Framework – Invitation to Tender

This has been a common issue – in some cases it has simply been a matter of configuring existing software; in others new software has been required. The DWP Departmental Security Team (DST) have been very clear in that Encryption **must** be in place before access to DWP data and to Provider Referral and Payment System (PRaP) is granted.

5 Penetration Testing

The DWP requires that a comprehensive Penetration Test, conducted by an independent reputable company, is undertaken before access to DWP Data and to Provider Referral and Payment System (PRaP) is given and any processing of any PRaP Provider Information on PRaP Provider Information Systems and Services takes place. For clarity this is the completion of testing, reporting and addressing vulnerabilities identified.

5.1 Timing

From experience, some Providers have planned the necessary testing but have scheduled it to take place after the systems are in live operation and processing referrals. The DWP Departmental Security Team (DST) have been very clear in that the Penetration Testing, and all necessary remediation of discovered weaknesses, **must** take place before access to DWP data and to Provider Referral and Payment System (PRaP) is granted.

5.2 Scope

The DWP have been asked what the scope Penetration Testing should cover. As this may vary between Providers, due to having different PRaP Provider Information Systems and Services, we have provided general guidance on scoping the testing required, embedded below:



Provider Penetration
Testing Guidance

Providers are encouraged to share this Provider Penetration Testing Guidance document with their prospective Penetration Testing supplier(s), to assist with consistency across quotations, and to share proposals from their supplier with DWP ahead of testing, to reduce the risk of additional testing being required due to gaps in scope.

5.3 Choosing a Supplier

The DWP requires Providers to use an independent reputable company to undertake their Penetration Testing to commercial best practice. This means that it should be an external company not providing systems or services connected in any way with the PRaP Provider Information Systems and Services, and they should be recognised as experienced specialists in this field.

PROTECT – COMMERCIAL

Department for Work and Pensions – The Framework – Invitation to Tender

It is expected that a reputable company and / or their staff would be a member of a recognised scheme for trustworthy and professional penetration testers, which require members to pass various standardised tests / exams and maintain certification credentials. The DWP require Providers to use a penetration tester who has passed a technical test approved by CESG; currently, this includes:

CHECK – http://www.cesg.gov.uk/products_services/iacs/check/

CREST – <http://www.crest-approved.org/>

TIGER Scheme – <http://www.tigerscheme.org/>

and it is likely that they follow one or more testing methodologies, such as:

OWASP – <http://www.owasp.org/>

OSSTMM – <http://www.isecom.org/osstmm/>

Other schemes, qualifications and methodologies exist, which may or may not be relevant to the scope of testing. Providers should contact DWP if any doubt exists as to the suitability of any company to meet the requirements.

5.4 Remediation Plan

After the Penetration Testing results have been received and reviewed by the Provider, the DWP requires a Remediation Plan, along with the Penetration Testing results, detailing how and when the Provider will address each of the findings raised by the testers. This is to ensure that the Provider both understands the risk posed by the vulnerability and mitigates it to that satisfaction of the DWP. The Department may withhold any data and PRaP connection until completed and approved.

Experience has shown that a spreadsheet, detailing test reference, vulnerability, impact / criticality, proposed / completed remediation action, and target date helps with the process, especially where remediation is tracked and reported over a period of time due to time required to implement.

NB Where a Provider records and tracks their risks in a Risk Register, this is often the ideal place to record the penetration testing findings and identify their Risk Treatment.

5.5 Remediation Evidence

Where Penetration Testing highlights an issue, which must be addressed through the Provider's Remediation Plan, the Provider is expected to supply evidence in support of their remedial actions. This may be in the form of screenshots / photos, updated documentation, written confirmation / assurance, a site visit by the Security Assessor, or an independent retest by a penetration tester. What evidence is required will be determined, on a case-by-case basis, by the DWP after communication with the Provider.

PROTECT – COMMERCIAL

Department for Work and Pensions – The Framework – Invitation to Tender

6 Advice and Guidance

Once a Provider has been chosen as a Preferred Bidder, there is scope to engage with the DWP Security Assessment Team to obtain advice and guidance in relation to the Provider's PRaP Provider Information Systems and Services. Advice and guidance will naturally have limits, as design and policy development is the Provider's responsibility and the Security Assessor cannot get into a position where they might review their own work.

Where a Provider has limited knowledge, experience and / or resources to address the information security requirements of the contract in-house, we recommend that they seek external professional support at an early stage. Support may include assistance in areas including secure network design and system build; development of information security policies and procedures; management and monitoring of systems and security devices.