Cabinet Office

PSN
Public Services Network

PSN IA conditions supporting guidance

Guidance
July 2012
version 1.4

Introduction

This document provides guidance on achieving compliance with the PSN IA conditions (Ref [ST09]). The PSN IA conditions is a framework of controls that must be applied by any organisation wishing to connect and/or consume PSN services.

These requirements are intended to provide a minimum set of baseline connection standards for all organisations. These minimum standards are essential to enable all organisations using this shared service to have confidence that risks are being appropriately managed.

Context

These controls are designed to reflect good practice that, for the most part, would be required by any organisation to show due diligence and prevent any claims of negligence against its senior management. They include controls that are intended to address the requirements of the following where appropriate:

- Data Protection Act (see BSI BIP 0012)
- Human Rights Act (Right to privacy)
- HMG Security Policy Framework
- Accountability of users (Computer Misuse Act also see BSI BIP 0008 and BS 10008)
- Risk management (See HMT Orange Book and ISO/IEC 27005)
- Corporate Governance (Audit commission Report on Corporate Governance in the Public Sector)
- Official Secrets Act (with regard to Protectively Marked information)
- ISO/IEC 27001 (Information Security Management System Requirements)
- Local Government Data Handling Procedures

There is a significant amount of guidance available, CPNI Guidance, the CESG policy portfolio, ISO/IEC 27002, CobiT and various others, which are proven and respected. Organisations should refer to these when assessing whether the controls that they have implemented are adequate and cost-effective.

Information Assurance is intended to support the organisation and enable business. Its purpose is to ensure that information is available to the right people when needed and to maintain the integrity of that information. This is a basic tenet of good operating practice.

In general, where organisations are already following good practice, compliance with the IA Conditions should not lead to additional work or cost. If good practice is being followed then this can be reused to demonstrate IA Conditions compliance. However, if the customer does not implement the practices required by the PSN IA conditions as part of their existing approach then additional controls will expected to be implemented to gain PSN IA conditions compliance.

There should be minimal need to implement additional controls unless Public Sector organisations are currently missing or are not adequate and justification for new or modified controls should be more than the need to meet PSN obligations. These controls

should help improve and maintain the overall Information Assurance and Risk Management of the Public Sector.

Compliance with the IA conditions will help to provide confidence to the general public that they are handling their information in an appropriate and safe way.

Definition

In order for a customer to obtain PSN compliance the organisation must comply with the PSN Code of Connection (Ref [ST11] [FO01]). The code of connection incorporates several control objectives including aspects of governance, technical interoperability requirements, service management expectations and Information Assurance (IA) standards. This document provides Public Sector organisations with guidance on how to successfully comply with the IA requirements known as 'IA conditions'.

It is essential that the IA conditions are not seen as a simple tick sheet. The IA conditions are a risk management tool to be used by customers to enable the PSN team to understand the level of risk that a connecting organisation introduces to the PSN. Risks can be mitigated in a number of ways, and therefore the IA Condition controls are as outcome focussed as possible, enabling the customer to implement suitable and effective IA controls.

Compliance with the IA conditions, as part of the CoCo is assessed by the PSN team in line with PSN Compliance document (Ref [ST09])

Intended Audience

This document is to be used by an organisation aiming to achieve compliance with the IA conditions, which forms part of the PSN Code of Connection. This document provides additional context around the control statements and offers support in meeting the IA conditions control objectives.

The IA conditions are provided for customers at operating between IL0 and IL3. The IA controls are identical at each impact level; however, the application of those controls may vary. Where appropriate, additional guidance is offered to distinguish how the application of those controls may vary.

Updates

This document and the IA conditions will be subject to review. The PSN Security Forum will review the IA conditions on an annual basis to refine existing controls sets, add new controls to address specific IA challenges and remove controls that are no longer relevant.

To support updates it is expected that a roadmap will be developed to highlight the future direction of the IA conditions, for example to phase in additional controls. A roadmap will enable customers/organisations to understand the implications of future changes

This document is under the configuration control of the PSN team, and will be changed in accordance with PSN Document Management and Change Control (ref [ST07])

How to apply the IA conditions

IA conditions structure and scope

The IA Conditions takes the form of a number of IA Controls divided into relevant subsections such as physical security or Incident Management.

The IA Conditions are all mandatory unlike other Codes of Connection where there are often distinctions between ‘Must’ and ‘Should’ controls. It is for each connected organisation to display compliance against each condition, or to prove that a Condition is not appropriate or that the risks addressed by the condition are met by other mitigations. The PSN IA conditions have been created to specify minimum security requirements for organisations accessing PSN services, other requirements are not within scope.

The organisation is required to effectively scope what is within the PSN and subject to the PSN Conditions. The IA conditions do not need to be in scope for equipment or people that do not access the PSN when separation of that activity is assured. This approach enables organisations to connect to and consume PSN services from an enclave where needed, rather than allowing access from across the entire ICT estate.

Within scope, as a minimum any device, network, person or physical location that connects to or accesses PSN Services that are not already PSN Certified must be considered as targets for compliance.

Control DIA.1 (Network Diagrams) should be used to highlight what areas are considered in or out of scope for the PSN IA conditions assessment.

It is accepted that there are potentially cases where PSN services are accessed from PSN accredited and assured equipment in its totality. In this instance it is likely that the technical controls will already be applied and the organisation will only need to scope the physical and personnel security controls.

Once the scope is clear the customer organisation will need to apply all of the controls within that scope. It is accepted that organisations may already have certain controls in place, or that they might not be applicable as the services are pre-approved and supplied through the PSN. Where this not applicability occurs supporting comments must be provided to explain the reason why.

The Conditions are aligned with established good practice, and are broadly consistent with the controls detailed in ISO/IEC 27001.

The IA Conditions request evidence in the form of policies or documents. These documents are named (e.g. removable media policy). The name of the document is not important; in order to be compliant an equivalent document with alternative name can be used. It is the outcome that matters, not the document name. Documentation being used as evidence should be referenced within the comments section of the IA Conditions.

The following section provides further guidance on applying this individual IA Conditions.

Subject specific guidance

DIA.x Network Diagrams
Explanation:
An up to date high level/logical network diagram is fundamental to understand the connection environment. The high level diagram is not expected to include every last device, in fact the diagram can be conceptual, but is required to ensure that the scope of the connection is understood by the customer and anyone carrying out a compliance check. The customer environment may be very complex with a mixture of services being consumed some will be PSN branded services and others locally procured or implemented. The key aspects to be included are: - Service interaction, so it is clear which services the organisation is consuming and whether they are PSN or non PSN services. The outcome is to highlight where service interact or interoperate. - Context around onward connectivity. If the organisation has onward connections to systems/services/networks that are either PSN or non PSN networks. Onward connections may also include detail around where the gateway is positioned. - Any off shoring of systems and information, including any life support/maintenance connections - Third party connectivity
Guidance:
[DIA.1] As a minimum the diagram will include: Organisational name, date of diagram, author, security domains/environments (e.g. RESTRICTED or IL3 Domain), local connections (with approximate numbers of users, PSN services, Non PSN Services, remote connections/access, all external and third party connections (with names of organisations, impact levels of connection, business reason for connection and boundaries of responsibility), location of security devices such as gateways (it is accepted that not all devices will be included but those that the customer may wish to highlight later in the various controls should be included), wireless network devices, infrastructure or connections that are off shored. It is not necessary for organisations to include the details of services and equipment that has already been accredited by the PSN, simply to show connections to them. Where appropriate, for larger and more complex configurations, it is not expected that every connected device be shown. A realistic level of abstraction can be employed for standard builds and configurations, to ensure clarity around connections, security domains and services. Abstraction should be used to make the diagram simpler to produce and review. It might be appropriate to group assets by business impact level or function. The diagram method itself is not stipulated, some organisation may consider using the IS1 modelling methodology (Ref [E3]) others a more technical diagram. Due to the level of detail required, this diagram may require protectively marking. [DIA.2] The customer understands that compliance of the IA Conditions allows them to use the PSN to share information across the PSN with other PSN connected organisation and consume PSN approved services. However customers are not permitted to expose non-PSN approved services to the PSN unless these have been assured and offer protection to the rest of the PSN. An example might be the wider sharing of an organisational developed service such as an HR function from one customer to other PSN connecting customers. Any service delivery of this type will need to be in accordance with the PSN Compliance document (Ref [ST09]) that places

restrictions around the scale, scope and appropriateness of this type of service delivery. Any onward services will need to be included in scope of the PSN IA conditions submission for assessment.

The actual assurance requirements may vary, and therefore it is recommended that any customer intending to offer services in line with the PSN Compliance document seeks advice from the PSN team.

RIS.x Information Risk Management

Explanation:

Risk Management is fundamental in enabling organisations to identify and mitigate risks appropriately. One of the fundamental tenets of the IA Conditions is that consuming organisations are operating under the principles of a risk managed regime.

When performed correctly, Risk Management enables an organisation to understand a system, and the possible impacts that may result due to a risk being realised. This will allow for the application of appropriate risk mitigation techniques.

Guidance:

[RIS.1] IA Conditions submissions shall include a description of the risk management process or methodology employed by the organisation. To comply with the IA Conditions organisations shall demonstrate that information security decisions should be risk based and the application of appropriate mitigations is appropriate to the risk.

Where SPF compliance is mandated, HMG IA Standard No. 1 (IS1) Part 1 Technical Risk Assessment (Ref [E3]) should be used for Risk Assessment, and IS1 part 2 used as guidance for Risk Treatment (Ref [E3]).

For organisations not subject to the SPF, IS1 remains relevant and should be consulted. Alternative methodologies may be appropriate.

A register of information assets should be maintained to include identification of individual assets or groups of assets and specific ownership of those assets.

Information classification and handling policies are defined to include legal requirements, sensitivity and criticality and an appropriate set of procedures are be developed and implemented to ensure that information assets are managed in line with these policies.

[RIS.2] Organisations should also be able to explain the governance of the ICT system which they are connecting to the PSN. There should be an individual or committee at Board level that is responsible for accepting or rejecting risk balancing business requirements and advice from security staff.

PHY.x Physical Security

Explanation:

Whilst the majority of the PSN IA conditions focus on data protection and technical measures, assets that process and/or hold data also need protecting from physical compromise, theft or tamper. They should be located in a secure location that offers adequate protection.

Guidance:

Physical security of equipment should be included within the overall risk management process.

The connecting organisation shall ensure that physical access to the buildings and rooms holding PSN equipment is commensurate with the data held and in accordance with the organisation's risk management approach. Departments should consider producing an Operational Requirements statement.

Other sources of advice include:

- CPNI Physical Security Measures
- CPNI Guide to Producing Operational Requirements
- CPNI Good Practice Guide Telecoms Resilience
- CPNI Good Practice Guide Protecting Data Centres
- Security Policy Framework (Physical Security)

CPNI documents can be found at the CPNI website (www.cpni.gov.uk), under the Physical and Information Security headings.

PER.x Personnel Security

Explanation:

Personnel security measures help organisations manage the risk of staff or contractors exploiting their legitimate access to their premises, information and staff for unauthorised purposes. It is important to ensure that the users accessing data and those responsible for administering the systems have their identities and backgrounds verified to mitigate against the risk of employing people with a criminal background or those who do not have the necessary qualifications or experience for the job. These issues are not just resolved during the recruitment process; personnel security is a discipline which needs to be maintained throughout the whole period of employment. Included should also be a formal process for managing staff leaving the organisation.

Guidance:

The Baseline Personnel Security Standard (BPSS) provides a level of assurance of the trustworthiness and integrity and probable reliability of prospective employees. It is closely aligned to recognised good practice such as BS7858.

Personal security checks and monitoring should be ongoing processes, to help identify changes in behaviour and/or circumstance that may be of concern.

Additional details can be found at the following:

- Cabinet Office Baseline Personnel Security Standard
- CPNI Website, covering topics such as:
  - Managing Contract Staff
  - Ongoing Personnel Security
  - Overseas Criminal Record Checks
  - Security Culture

All staff that have access to PSN services or networks either directly or through an application presented to a lower classification domain are required to undergo the BPSS or equivalent check.

A BPSS check involves verification of:

- Identity.
- Employment history (past 3 years)
- Nationality and immigration status (including an entitlement to undertake the work in question)
- Criminal Record (unspent convictions only)

It is strongly advised to engage your Human Resources department when implementing this control. Additional guidance on managing personnel security can be found at the CPNI public website.

EDU.x User Education

Explanation:

User education is a fundamental step in mitigating many of the threats to ICT systems. If users have not received sufficient training it is unlikely that they will understand and comply with all the restrictions and responsibilities which are placed upon them, or be in a position to identify anomalous activity.

Guidance:

[EDU.1] User education should include the following:

- Ensuring all users have read and understood all user security requirements including the Organisational Security Operating Procedures (SyOps) and incident reporting processes.
- Legal restrictions and responsibilities (e.g. Data Protection) and business controls before access to information or services is granted.

In addition users are expected to understand how their actions or inaction could affect an ICT system.

Organisations should also provide details to the compliance team on the dissemination of updated security procedures and guidance for users that enable them to receive the latest available information in a timely manner. It is recommended that such procedures will frequently be distributed as part of a broader awareness strategy.

[EDU.2] Suitable evidence to achieve compliance in this control will include the user being presented with an “An Acceptable Use Policy”. Users positively confirm their acceptance of the policy and that communications sent or received by means of the PSN may be intercepted or monitored.

Some sample text for the customer organisations acceptable use policy can be found in Appendix A. It is accepted that many organisations already have similar user statements. The way in which the policy is implemented is at the organisation’s discretion. It could be implemented via documentation, in soft or hard copy, or electronically (for instance by getting a user to verify they have read and accepted the organisation’s policy by clicking on a box on their start up screen). However the policy is implemented, the Risk Manager will ensure that users of the PSN are fully aware of their responsibilities. The Risk Manager may also wish to seek advice from the relevant Human Resource and Legal advisors in their organisation.

RES.x Incident Response

Explanation:

Incident Response procedures are crucial for the management, monitoring and resolution of security incidents. Effective incident response procedures can help identify and contain anomalies and assist with recovery from them. Finally, developed Incident Response procedures will assist an organisation to identify recurring or related incidents, though incident recording and review.

Guidance:

Organisations will have an Incident Response policy in place that includes:

- Security Incident Monitoring and Alerting
- Security Incident reporting
- Security Incident classification
- Defined roles and responsibilities for Incident Management.
- Procedures for escalating Incidents to the PSN team.
- Post incident review

For HMG it is a requirement of the SPF (MR 12) that all security incidents be reported to an appropriate departmental security authority and GovCertUK. It is likely that most organisations will not have a specific Incident Response policy for PSN, but have generic policies which are applicable to their PSN connected equipment and services.

The guidance below gives additional advice on the reporting of security incidents and Incident Management:

- GovCertUK Web pages (reporting an incident)
- CINRAS - IA Standard 4 Supplement 11.
- WARPS (Warning, Advice and Reporting Points). Details can be found at the WARPS website.
- CPNI Technical Note 01/2005 – An introduction to Forensic Readiness Planning
- CESG Implementation Guide 18 Forensic Readiness Planning
- CESG Good Practice Guide 18 Forensic Readiness
- FIRST - Forum of Incident Response and Security Teams. Details can be found at the FIRST website.
- CESG Good Practice Guide No. 24 Security Incident Management
- Cabinet Office Guidance on notification of breaches of a classified nature
- Cabinet Office: Reporting of data breaches of an unclassified nature

CON.x Configuration

Explanation:

The PSN does not stipulate a specific configuration requirement; it expects that the organisation will develop internal policies that demonstrate how their risks are being managed.

A well configured network will be security hardened to minimise services that may be exploited by an attacker. Configuration control is essential to ensure unauthorised changes cannot take place or are detected.

Whilst best practice IA guidance encourages minimal services and software, it is recognised that actual configuration will be designed to enable business functions. However, it is important that the risks of running certain software configurations or services be fully understood and managed.

Guidance:

[CON.1] Organisations should apply lockdown policies for network connected equipment. Where lockdown advice is not available for a particular product or platform, the vendor should be consulted. Any policy is expected to highlight how risks are being managed.

IL3 Note: It is recommended that the GAP (Government Assurance Pack) lockdown should be deployed to Windows clients that are being used at IL 3 and above. GAP is a best practice framework developed by CESG for configuring and securing Windows client operating systems. The purpose of the GAP lockdown is to improve the default security configuration in windows and provide mitigations against malicious software, remote attackers and hostile users which are the three principal sources of security threat to computer systems in high-value security environments.

For networks that are operating at IL 2 and below, it is recommended that industry best practice such as Microsoft's SSLF and software restriction policies such as AppLocker should be applied.

In a server environment the threat from the standard user is mitigated as standard users should not have regular access to the server OS. Instead, it is usually the case that the Server is accessed for Administration and would require Administrator credentials – this would bypass a lot of traditional lockdown features. In order to lockdown a server environment it is recommended that a secure configuration such as Microsoft's SSLF is applied as well as following best practice such as removing and restricting programs and services that are not required for business use.

Where appropriate, 'build images' should be created to ensure a known configuration is deployed.

[CON.2] [CON.3] In order to achieve effective configuration control Public Sector organisations will consider what limitations are required on software usage. Permitting users to install software that is not controlled will bring risk to the connected organisation and the PSN. The risks of allowing the use of unsupported, non corporate standard and/or unofficial software should be managed. Risk management should consider that allowing this software may prove difficult to keep up to date and vulnerabilities left un-patched.

All security settings should be documented and understood, and any deviations approved. Where changes are necessary, a detailed and rigorous change control procedure should be followed to ensure all changes are fully documented and approved.

Restricting changes to the configuration of equipment should include procedural and technical measures. Users should be instructed as to the risks or non-standard software, and restrictions should be clearly stated within the user SyOps.

Deviations from standard configurations, and unauthorised changes should be detected, either through monitoring, file integrity checking, regular reviews or IT Health Checks.

Where possible, the latest versions of software, service packs and updates should be used at the earliest opportunity. These should include the latest security updates. Older versions of software may be out of support, and security updates may not be available.

[CON.4] Privileged accounts should only be used for activity that requires that level of privilege. Many attacks enable an attacker to run code in the context of the currently logged in user. If that user account is privileged, the impact is higher.

An attacker, having gained a foothold within a network, will seek out privileged accounts. If these accounts are poorly controlled, the attacker's task becomes easier.

[CON.5] Active content is data that requires some sort of execution during rendering so that it can be displayed properly. Examples include JavaScript, Adobe Flash and Microsoft Office Macros. Access to this sort of content should be restricted if it is not required.

Additional Advice can often be obtained from the following:

- CESG – GAP FAQ
- CESG – Using Windows in High Security Environments
- NSA – Security Configuration Guides
- NIST - Security Configuration Guides

CHE.x Compliance Checking

Explanation:

It is extremely important to ensure that the operating systems, software and hardware are configured securely when they are installed and that they are patched regularly.

As new vulnerabilities are being discovered by security researchers on a daily basis, and these are quickly used by attackers to attack systems, it is important to regularly review the security configuration to ensure that configuration and patching levels remain sufficient.

This is particularly important for PSN connected organisations that if compromised, may be used by an attacker to onwardly attack other PSN connected organisations.

An IT Health Check (ITHC) will help identify known vulnerabilities that an attacker may attempt to use to gain access to a system. An ITHC will use many of the attack techniques that a Hacker may use, and provides a more thorough evaluation of security than a vulnerability assessment.

Guidance:

It is important to understand the scope of this control. Compliance with this control does not mean organisation will be required to carry out ITHC on all devices. The important angle is that the organisation has an effective programme of ITHC in place that focuses on devices that connect to PSN equipment or consume PSN services. For large scale infrastructures it is expected that the ITHC programme will not always cover all devices annually but it is assumed that the scope of annual IT Health Checks will be cycled appropriately,

It is important to utilise experienced, impartial and suitably qualified security consultants for testing PSN connected equipment. These assessments may be supported by periodic validation by internal staff.

Cross checking the results of an ITHC against a baseline and previous assessments is one way to gain assurance that network security has not degraded over time, and that previously identified issues have been addressed.

It is important that all ITHC and vulnerability scans are correlated with the information available from Audit logs. This is to ensure that the activity generated by the tools used during the scans, many of which may also be used by hackers, are adequately recorded.

Organisations should analyse the results from the ITHC, to understand the risks associated with the identified issues. Where remedial work is required, an action plan should be developed (or added to the risk treatment plan) to ensure appropriate mitigations are deployed.

ITHC are required on a regular basis due to the changing nature of vulnerabilities and threats. In addition, the organisation itself may need to change the testing scope to focus on particular areas of concern.

Assurance of ITHC services can be obtained by using a company that is a member of CHECK or of a scheme such as CREST and TIGER that has a professional body. Details of CHECK approved providers can be found on the CESG website. Other bodies have their own websites

IL3 Note: For IL3 consumers, it is expected that IT Health Check s will be conducted by a CHECK approved service provider.

PAT.x Patch Management

Explanation:

New vulnerabilities in software and firmware are reported on a daily basis, by customers and Security Researchers who are constantly seeking them out. The time taken for exploits to be developed from these vulnerabilities is ever reducing and security updates, which aim to fix them, should be applied as soon as is reasonably possible.

Guidance:

A patch management policy sets out the principles behind applying patch updates. It should include details on prioritisation, testing, application, monitoring and scheduling. The policy should also include provision for the application of high priority security updates, for example ones that are released by the vendor to address issues which are actively being exploited by attackers.

It is important to note that the patching policy includes details for the application of all security updates, which is for all network devices and applications, and not just for the operating system.

It is strongly recommended that all patches be tested before application. Whilst vendors endeavour to test patches to ensure that they have no negative effect, it is up to individual customers to test all patches against their own configuration and software build.

Software that is no longer supported will become vulnerable, as patches will not be developed for known vulnerabilities. Supported alternatives should be used where available. Where supported software is not available a risk assessment should be undertaken and mitigating measures undertaken.

Additional guidance can be found in the following:

- NIST - Procedures for Handling Security Patches
- NIST - SP 800-40 Creating a Patch and Vulnerability Management Programme
- CESG Good Practice Guide 20 ICT Service Management: Security Considerations

ACC.x Access Control

Explanation:

Access to services should be for named individuals only, and be supported by a sufficiently robust access control policy that will include authentication requirements. In developing the policy it should be noted that weak passwords may be guessed or broken by an attacker, and poor password management may lead to a number of issues such as passwords being written down, or passwords being reset without user identification. It is therefore expected that a holistic approach to access control be implemented.

Guidance:

As part of an access control policy, the organisation should consider whether/how to restrict access to information by individuals that do not have a business requirement for accessing a system and its data.

It is imperative that user accounts are unique to enable the tracking of specific activity to named individuals. This supports the overarching PSN Situational Awareness requirements. The use of

shared user accounts for access to a particular system or application should only be permitted where there is a clear business requirement. This is usually where a particular job role requires a generic account. The organisation will demonstrate clear and auditable processes are in place to track such usage. The use of shared accounts may cause issues with accountability and the audit of user actions.

For all PSN connected organisations, the following technical measures should be considered as part of their password policy. This list is not necessarily prescriptive but would represent a password policy in line with good practice:

- A minimum of seven characters;
- Use a complex character set that has at least one non-alphabetic character
- Changed a minimum of every 90 days
- Not reused within 20 password changes

Procedural measures should be in place to ensure:

- The user does not use any part of their individual account name
- The user does not reveal their password to anyone
- The user does not write down or display their password in their work area or any other place.

Organisations working at IL3 should follow the guidance linked below:

- CESG Implementation Guide no. 3 – User Authentication Systems
- HMG IA Standard No. 7 (IS7) – Authentication of Internal Users of ICT Systems Handling Government Information (Ref [E3]).

BOU.x Boundary Controls/Gateways

Explanation:

Whilst connections between systems are a required aspect of many business activities, the passing of data between systems poses risks such as the import of malicious software, or the leakage of confidential information.

This is most critical when implementing a gateway to a lower security domain. The lower security domain may not have sufficient risk management in place that a higher security domain may demand. For example it may have a less rigid removable media policy, or onward connections not appropriate for a higher security domain. In this way the lower security domain may become compromised, and lead to onward compromise of any connected system including the system in the higher security domain.

Controls need implementing on the automatic forwarding of email to ensure protectively marked emails are not forwarded to an unaccredited or private network.

Guidance:

[BOU.1] [BOU.2] [BOU.3] All services offered to external parties should be documented, and assessed in terms of risk, to allow appropriate mitigations to be employed. This includes connections to PSN, and non-PSN services.

[BOU.4] All services traversing network boundaries should be kept to a minimum to those necessary for business functions only. This reduces the opportunities for exploitation or mis-configuration that may be available to an attacker.

[BOU.5] All services to less trusted networks, i.e. those outside of the PSN, should pass through a content-aware proxy server, or be subject to content scanning to detect malicious activity and

policy violations. This includes email, web and file transfer activities. Where traffic cannot be inspected (i.e. it is encrypted in transit) the organisation should demonstrate an understanding of the risk that this represents and consider alternative appropriate measures.

This can help to prevent or detect for example, protocol tunnelling, unauthenticated users or programs accessing the network service, and makes it easier to spot egress of classified material to inappropriate destinations. The proxy can also provide logging facilities, and can help protect the network from certain types of buffer overflow attack.

Proxy servers should consider the need to authenticate both the user and, where possible, the (internal) host with which they are communicating, for example, by IP address and all PSN bound email should be routed to a PSN endorsed mail relay.

Due to the fallibility of Anti Virus software, it is strongly recommended that products from different vendors be implemented at different points in the network, i.e. on the Gateway device and on the desktops.

[BOU.6] White listing is an effective tool for limiting the file types that are permitted to cross the boundary. White listing specifies which file types or addresses are permissible. If managed correctly it can be effective, but is very restrictive on user activity. Black listing is also an appropriate consideration for gateways and boundaries. Black listing may specify which file types or addresses are not permissible. As such it is less restrictive and may require increased support due to the need to maintain the list of known 'bad' addresses.

It is important that all devices that together form the 'Security Boundary' or 'Gateway' are suitably configured. Advice on secure configuration should be obtained for all network connected devices, and this is most critical for those devices that have security functions between the PSN connected network and other security domains.

Previous guidance on the configuration of Firewalls is still relevant for Boundary and Gateway protection, and all gateways are still expected to be assured by a suitable mechanism, depending upon risk and function.

For reference, the recommended PSN firewall rule can be found within Appendix B.

For More details, refer to:

- CESG Good Practice Guide 8 - Protecting External Connections to the Internet
- CESG Good Practice Guide 35 - Protecting an Internal ICT Network

MED.x Removable Media
Explanation:
Removable media provide a simple method of data import and export, and as such pose risks for unauthorised data transfer. Users frequently use removable media to support home working or data sharing. Such activity indirectly connects the trusted network with other networks for which there may be very little security consideration. Removable media is a mechanism frequently associated with the introduction of malicious software, and could lead to system compromise and potentially impact any connected networks such as the PSN. Where removable media is required, policies should be developed to provide user guidance and to manage the resultant risks. Removable media also exacerbates the problems of controlling and tracking sensitive data. Not only can the devices store large quantities of data, they are also easily lost.

Guidance:

Organisations shall be able to demonstrate an understanding of the risks being exposed when permitting removable media to be used with any ICT system. Procedural and technical controls should be considered. Removable media users should be instructed in the risks of using unauthorised media, the physical protection of media, the steps required to import data from the media i.e. Anti Virus scanning and the data that is permissible to be copied onto that media.

Technical controls can include disabling devices e.g. through Group policy to disable USB, or through products that only allow the connection of authorised devices.

MAL.x Malware Protection

Explanation:

Malicious software (Malware) can affect the confidentiality, integrity and availability of data, for example malware can make sensitive data available to unauthorised persons for reading, modification and export, and it could lead to a loss of service. As PSN is a large scale shared service, any compromise can have a wide ranging impact.

Once Malware has been imported to a system, it may onwardly infect other devices or serve as a jump point for an attacker to onwardly compromise other systems.

Guidance:

All data imported to the organisation should be scanned for Malware, file verification and/or content that breaks the corporate policies or guidance.

This will include email and web traffic, data imported via removable media, or data originating from any other connected device or network. Options in this space include protocol checking, stateful firewalls, content analysis and the checking of encrypted content.

It is crucial that all scanning software is kept up to date with the latest definitions that are available, with some Anti Virus vendors updating their products multiple times a day. All updates should be obtained from trusted sources only.

Devices should be configured not to 'auto-run' content from externally connected devices or media and to automatically virus scan media when it is connected.

Malware protection is linked to configuration and patch management. By not running unnecessary services, the surface area of the device that may be compromised is reduced. The application of security updates will reduce the number of known vulnerabilities to which a device is subject.

Where the configuration and patch levels of devices can be verified on a regular basis, for example to ensure that all patches are being deployed and any unauthorised changes are detected, additional assurance can be gained.

[MAL.3] A "Stand alone virus checker" can be defined as a machine that has no direct connectivity to the operational network or systems. The sole purpose of this device to check removable media for malware and other content inspection as relevant before connecting the media to an operation network or system. The stand alone system should be managed to ensure that it is regularly subjected to updates. Ideally the stand alone system will have multiple methods for checking malware i.e. through the use of several ant-malware engines. The stand alone system will be expected to form part of the overall removable media/malware policy of the organisation.

For More details, refer to:

- CESG Good Practice Guide 7 – Protection from Malicious Code

MOB.x Mobile / Home Working

Explanation:

Mobile working is fundamental to the modern workplace, and may be central to the organisation's Business continuity plans. However mobile devices allow trusted networks to be accessed from environments over which the organisation has little or no control e.g. public places. The devices themselves may be lost or stolen, data may be read by uncleared individuals for example via 'shoulder surfing', and the devices could be used to attack the internal network.

Guidance:

CESG Good Practice Guide 10 gives advice about the risks and appropriate measures to manage remote working at a number of impact levels. Organisations are reminded that GPG10 (Ref [E5]) covers both technical and procedural guidance on remote working, and a purely technical remote working policy will not in itself be acceptable.

A remote working policy needs creating and all users need to be aware of the guidance and restrictions which it contains. This should include personnel and physical security aspects of using devices to access protectively marked data from public places. For example it should include advice on the storage of the device, its usage, method of connection to the internal network, password policies and restrictions for its use overseas.

Organisations should be able to specify minimum requirements for all remotely connected devices. As with any endpoint, mobile devices should run Anti Malware software and be securely configured, as described under 'Configuration' (above). They should also run a personal firewall and all relevant security patches should be applied.

In addition, these devices should employ appropriate encryption for data at rest and in transit. Details of suitable encryption standards can be found in Information Standard No. 4 (IS4) Management of Cryptographic Systems (Ref [E5]).

The use of mobile devices to access PSN services from overseas changes the nature of the risks to which those devices may be exposed. Organisations should develop specific policies and guidance where overseas working is a requirement.

IL3 Note: Devices used for remote and home working must implement appropriate encryption for data at rest and in transit in line with the SPF. Current requirements at IL3 require CESG Baseline approved products for encryption. All organisations should consider the appropriateness of encryption overseas and national legal restrictions.

WIR.x Wireless Networks

Explanation:

Many data thefts and compromises have occurred as a result of attackers gaining access to an internal network via a Wireless access point. The attacker is frequently located offsite; therefore they do not require physical access to the building containing the network which they wish to compromise.

A related issue is the security of Wireless clients which may connect to untrusted access points. Once compromised, these clients can be used to attack and compromise the internal network.

Guidance:

CESG Manual Y gives guidance on how to configure a corporately managed Wi-Fi network and apply WPA2 encryption. At IL3 it is recommended that the customer's wireless network is a validated implementation of Manual Y.

CESG Good Practice Guide 10 gives advice on other wireless technologies, such as Bluetooth and is a source of additional guidance on remote working.

Network vulnerability scanning tools should be used to identify access points, and any unauthorised devices should be disabled immediately.

OBF.x Network Obfuscation

Explanation:

From the outside of a network, it can be very difficult to understand how to mount a successful attack. Any information that the network reveals about its hardware, software and configuration may be useful to an attacker. An attacker who knows very little about a network may have to attempt many different methods of probing and attacking to gain knowledge of and access to a network. This approach is quite obvious and may lead the detection of the attack.

An attacker who has been able to passively obtain information about a network (information which has been released to external sources legitimately) will be in a better position to identify vulnerabilities and utilise attacks which will increase their chance of success and a lower the chance of them being detected.

Guidance:

Consideration is to be given as to what information is released to external sources concerning the internal configuration of the network, the software used etc. This might be achieved by appropriate configuration of externally facing devices, to ensure they communicate with the minimum amount of information required. An example of which is 'Banner Grabbing'; a technique that attackers may employ to gather information about open services on a system. Once the attacker knows what software versions are running, they can identify any weaknesses.

Many legitimate applications will communicate with cloud based services as part of their standard functionality, for example antivirus products. Departments should follow CESG guidance (Ref [E5]) on traffic collection and monitoring in order to minimise any adverse effect of these communication.

PRO.x Protective Monitoring

Explanation:

Protective Monitoring comprises three core processes: Accounting, Auditing and Monitoring of ICT systems. It is one of the most useful forms of detecting and understanding anomalous events. Without such analysis, malicious activity may go undetected, or it may be impossible to understand or resolve security events adequately.

Protective Monitoring may encompass virtually every network device and application; however careful thought needs to be given to the volume of data produced and the analysis performed.

Guidance:

[PRO.1] Detailed guidance for organisations implementing protective monitoring can be found within CESG Good Practice Guide No.13 (Protective Monitoring for HMG ICT Systems).

Where GPG13 (Ref [E5]) is used the protective monitoring applied be consistent with the relevant baseline countermeasures set from IA Standard 1 Part 2 and the Controls associated with the appropriate Recording Profile set out in CESG Good Practice Guide No.13.

It is important that devices have enough storage space for the amount of logs that they are required to store. Depending upon the device or application, if log storage space is full it may either stop working or overwrite historic information.

There are numerous tools that can assist with the processing and analysis of audit logs. It is recommended that some form of automatic processing occurs to improve the speed of analysis, and thus improve the efficiency of response.

[PRO.2] The PSN team or a delegated authority may occasionally request logging information from an organisation connected to the PSN. Where legally acceptable and appropriate these should be made available to the PSN team. This will only ever be in connection with a serious incident – one that almost certainly has had an impact on the connected organisation. In such a situation it is likely that this request would be part of assistance being provided to the organisation.

Understanding and managing the use of IP addresses can help ensure appropriate routing of information, and reduce the chance of accidental information release. Static IP addresses can assist with protective monitoring and incident response as the identification of devices is more easily achieved and should be assigned for all devices where possible. It is accepted that this will not always be practical, and in these cases other methods of correctly attributing devices should be sought.

For More details, refer to:

- CESG Good Practice Guide 13 - Protective Monitoring for HMG ICT Systems
- CESG Good Practice Guide 18 - Forensic Readiness
- PSN Protective Monitoring Guidance –CHECK NAME – to be produced.

IL2/3 Note: The requirements within GPG13 (Ref [E5]) for IL2 and IL3 ICT systems differ. At IL2 GPG13 generally advises the application of the Baseline Control set, whereas at IL3 individual risks need assessing and appropriate controls implementing.

GPG13 also details differing requirements for log retention, analysis and incident investigation at the two impact levels.

EMA.x Email

Explanation:

Email is frequently used as a method of delivering Malware, that is within the email itself or an attachment, or to entice the recipient to click on a link that leads them to a website from which Malware is automatically downloaded.

The richer the mail format, the more functionality that is available for an attacker to exploit.

Guidance:

Users should be made aware of the need to consider what information is being released via email outside of the organisation's network boundary. Requiring them to add protective markings to emails will ensure they consider the content, and will assist with any technical solutions for monitoring that may be deployed.

It is each organisation's responsibility to manage its data, and they should consider requiring users to add security labels consistent with the Government Protective Marking Scheme to any email that

contains information attracting a protective marking, i.e. PROTECT or above. This will help to limit the likelihood of accidental release of sensitive information.

Where a customer decides not to implement a labelling scheme or policy this should be done so as part of their overall risk management approach.

Example Acceptable Use Statements

- I understand and agree to comply with the security rules of my organisation.
- For the avoidance of doubt, the security rules relating to secure e-mail and IT systems usage include:
- I acknowledge that my use of the PSN may be monitored and/or recorded for lawful purposes;
- I agree to be responsible for any use by me of the PSN using my unique user credentials (user ID and password, access token or other mechanism as provided) and e-mail address;
- I will not use a colleague's credentials to access the PSN and will equally ensure that my credentials are not shared and are protected against misuse;
- I will protect such credentials at least to the same level of Protective Marking as the information they may be used to access, (in particular, I will not write down or share my password other than for the purposes of placing a secured copy in a secure location at my employer’s premises);
- I will not attempt to access any computer system that I have not been given explicit permission to access;
- I will not attempt to access the PSN other than from IT systems and locations which I have been explicitly authorised to use for this purpose;
- I will not transmit information via the PSN that I know, suspect or have been advised is of a higher level of sensitivity than my PSN domain is designed to carry;
- I will not transmit information via the PSN that I know or suspect to be unacceptable within the context and purpose for which it is being communicated;
- I will not make false claims or denials relating to my use of the PSN (e.g. falsely denying that an e-mail had been sent or received);
- I will protect any material, whatever the sensitivity or protective marking, sent, received, stored or processed by me via the PSN to the same level as I would paper copies of similar material;
- I will not send information marked RESTRICTED or above over public networks such as the Internet unless approved encryption has been applied to it;
- I will always check that the recipients of e-mail messages are correct so that potentially sensitive or protectively marked information is not accidentally released into the public domain;
- I will not auto-forward email from my PSN account to any non-PSN email account;
- I will disclose information received via the PSN only on a ‘need to know’ basis;
- I will not forward or disclose any sensitive or protectively marked material received via the PSN unless the recipient(s) can be trusted to handle the material securely according to its sensitivity and forwarding is via a suitably secure communication channel;

- I will seek to prevent inadvertent disclosure of sensitive or protectively marked information by avoiding being overlooked when working, by taking care when printing information received via the PSN (e.g. by using printers in secure locations or collecting printouts immediately they are printed, checking that there is no interleaving of printouts, etc.) and by carefully checking the distribution list for any material to be transmitted;
- I will securely store or destroy any printed material;
- I will not leave my computer unattended in such a state as to risk unauthorised disclosure of information sent or received via the PSN (this might be by closing the e-mail program, logging-off from the computer, activating a password-protected screensaver, etc., so as to require a user logon for activation); and
- Where my organisation has implemented other measures to prevent unauthorised viewing of information displayed on IT systems (such as an inactivity timeout that causes the screen to be blanked or to display a screensaver or similar, requiring a user logon for reactivation), then I will not attempt to disable such protection;
- I will make myself familiar with the security policies, procedures and any special instructions that relate to the PSN;
- I will inform my manager immediately if I detect, suspect or witness an incident that may be a breach of security;
- I will not knowingly attempt to bypass or subvert system security controls or to use them for any purpose other than that intended;
- I will not remove equipment or information from my employer's premises without appropriate approval;
- I will take precautions to protect all computer media and portable computers when carrying them outside my organisations' premises (e.g. not leaving a laptop unattended or on display in a car such that it would encourage an opportunist thief);
- I will not knowingly introduce viruses, Trojan horses or other malware into the system or PSN;
- I will not disable anti-virus protection provided at my computer;
- I will comply with the Data Protection Act 1998 and any other legal, statutory or contractual obligations that my employer informs me are relevant; and
- If I am about to leave my employer, I will inform my manager prior to departure of any important information held in my account.

Recommended firewall rule set

From	To	Protocol	Action	Comment
Your proxy/NAT	PSN	HTTP (TCP/80) HTTP (TCP/8080) HTTPS (TCP/443)	Allow	Enable outbound access to applications within the PSN using HTTP & HTTPS
PSN	Your applications/Web servers	HTTP (TCP/80) HTTPS (TCP/443)	Allow	Enable inbound requests from the PSN to your Web Servers/ Applications
PSN	Your mail servers	SMTP (TCP/25)	Allow	Enable inbound email from PSN
Your mail servers	PSN	SMTP (TCP/25)	Allow	Enable outbound email from your network to the PSN
Your DNS Server(s)	PSN DNS servers	DNS (UDP/53) DNS (TCP/53)	Allow	Allow queries to the PSN DNS servers
Your NTP servers	PSN NTP Servers	NTP (UDP/123)	Allow	Allow queries to PSN NTP servers
Any	Any	Any	Block	Default rule for all other traffic.

IA conditions mapped against GSi CoCo

	GSi IL2	GSi IL3	PSN
Network schematic	Organisation commitment statement confirms that a schematic is provided.		DIA.1 High level / logical network schematic accompany the IA Conditions document.
Accreditation	Accreditation statement - approved security policy, a security management process and security operating procedures	Accreditation statement - accredited for RESTRICTED, a full RMADS in accordance with SPF and relevant HMG and CESG IA Standards.	RIS.1 Risk management and standards based approach to assurance
Governance	Cover sheet Risk owner identified Organisation and accreditation statements - SIRO and accreditor endorse the CoCo	Cover sheet SIRO identified Organisation and accreditation statements - SIRO and accreditor endorse the CoCo	RIS.2 Board level responsibility for information risk identified
Physical security	1.1 Hosts and network equipment in secure accommodation	1.1 Hosts and network equipment in secure accommodation commensurate with protecting assets carrying the protective marking of RESTRICTED	PHY.1 Equipment has physical security commensurate with the function. PHY.2 Access to buildings and rooms containing equipment and terminals is secured.
Personnel security	6.3 BPSS for all users who have regular access to RESTRICTED	6.3 BPSS for all users 6.4 RECOMMEND SC for some roles	PER.1 BPSS for all users
User education	2.1 Training and awareness 2.2 AUP		EDU.1 Training and awareness EDU.2 AUP
Incident response	3.1 – 3.3 Process to manage and report		RES.1 – RES.3 Process to manage and report
Secure configuration	4.1 Hardware and software	4.1 Hardware and software 4.5 RECOMMEND GAP	CON.1 Hardware and software CON.1 Recommend GAP
Unauthorised software	4.2 Execution prevented		CON.2 Execution prevented
Configuration control	4.3 Required		CON.3 Required
Least privilege	18.1 Web browser and web enabled applications		CON.4 User accounts
Active content	18.2 ActiveX, 18.3 Active content, 18.5 Java virtual machine, 20.1 Macros RECOMMEND that all are disabled		CON.5 Within the context of risk management
Executable content	21.2 RECOMMEND that automatic execution of email content is not allowed 21.3 RECOMMEND that executable attachments to email are not allowed		CON.6 Run with the user's active consent and within the organisation's control
Compliance checking	5.1 Annual ITHC	5.1 Annual ITHC 5.2 Use CHECK	CHE.1 Annual ITHC

	GSi IL2	GSi IL3	PSN
Patch management	14.1, 14.2 Patching policy exists and is applied		PAT.1, PAT.2 Patching policy exists and is applied
	6.1 Each user has a unique userid		ACC.1 Associate all activity with a unique user identifier
	6.2 Sufficiently complex passwords 6.5 File system access control	6.2 HMG policy compliant passwords 6.5 File system access control	ACC.2 Access control policy that manages risks
	16.2 Connection to lower domains appropriate controls 16.4 Connection to higher domains formal assurance	16.2 Connection to lower domains appropriate controls (slightly different wording) 16.4 Connection to higher domains formal assurance	BOU.1 Assured mechanism between different impact level domains
	8.2 EAL4 firewall between organisation and third parties. RECOMMEND that it is different to the firewall between organisation and GSi.	8.2 EAL4 firewall between organisation and third parties. Different to firewall between organisation and GSi.	BOU.2 Assured gateway between PSN and non-PSN
			BOU.3 Effective mechanism between same impact level domains
	8.3 Configuration of firewall between organisation and GSi		BOU.4 Minimise services between domains
	17.4 RECOMMEND protocol checking by proxy servers 19.2 Content analysis of all traffic including virus check email and attachments at gateway and host 19.3 RECOMMEND gateway and host use different content analysis software 21.4 RECOMMEND encrypted files not sent by email 21.5 RECOMMEND email attachments and extensions validated		BOU.5 Content analysis of all traffic between PSN and non-PSN including virus check email and attachments at gateway and host
	19.4 RECOMMEND white list of allowed attachment file types		BOU.6 White list of allowed attachment file types
Removable media	15.1 RECOMMEND access disabled 15.2 RECOMMEND handle in accordance with HMG policy	15.1 RECOMMEND access disabled 15.2 Handle in accordance with HMG policy	MED.1 Policy must be within the context of risk management

	GSi IL2	GSi IL3	PSN
	17.4 RECOMMEND protocol checking by proxy servers 18.4 RECOMMEND https is disabled 19.2 Content analysis of all traffic including virus check email and attachments at gateway and host		MAL.1 Identify malware and vulnerability exploiting code at the gateway. End point equivalent when encrypted
	19.1 Identify and isolate malicious software		MAL.2 Identify and isolate malicious software
	19.5 Content analysis for removable media		MAL.3 Content analysis and AV scan of removable media; ideally on a stand alone virus checker i.e. a machine that's sole purpose is to check removable media for malicious content and is isolated form, the main network/infrastructure.
	10.1 Operate in accordance with HMG policy and guidance 10.4 Only connect from official / managed devices		MOB.1 Operate in accordance with the organisation's remote / mobile working policy.
	10.3 PED in accordance with CESG guidance 10.5 Personal firewall		MOB.2 Appropriate control and management of the technical environment.
			MOB.3 Organisational lockdown and configuration management policies for mobile / remote devices.
	10.6 Two factor authentication		MOB.4 Two factor authentication
	10.2 Encryption to protect data at rest and in transit. CAPS, other CESG approval for RESTRICTED, or FIPS-140	10.2 Encryption to protect data at rest and in transit. CAPS or other CESG approval for RESTRICTED	MOB.5 Encryption to protect data at rest and in transit with a suitable level of assurance.
Wireless networks	11.1 In accordance with Manual Y or other approved encryption. Include in ITHC		WIR.1 Policy in line with public sector guidance.
Network obfuscation	12.1 Minimise details of internal network structure, components and security tools and techniques that are passed outside the organisation 12.2 NAT 12.3 RECOMMEND PAT		OBF.1 Minimise details of internal network structure, components and security tools and techniques that are passed outside the organisation
	13.1 Protective monitoring controls in accordance with GPG13. Apply GPG 13 Baseline Control Set 2	13.1 Protective monitoring controls in accordance with GPG13. Apply GPG 13 Baseline Control Set 3	PRO.1 Protective monitoring controls commensurate to environment and data processing requirements. Good practice guidance in GPG13.

	GSi IL2	GSi IL3	PSN
	13.2 Audit logs available to assist in investigations and access control monitoring 13.4 Provide logs on request		PRO.2 Subject to legal constraints, provide information and make available audit logs
	13.3 Logs maintained for a minimum of six months		PRO.3 Within legal constraints retain audit logs for a minimum of six months.
	13.5 Common time source; GSi time source preferred		PRO.4 Consistent time source synchronised across all devices. The time source applied shall support effective log analysis and be from the time source of their PSN Service Provider.
			PRO.5 Possible to match server activity to a specific server.
Email	23.1 The mail client or user adds security labels to each email that carries a protective marking of PROTECT or higher		EMA.1 Emails and attachments labelled to highlight the sensitivity and value that the information has to the data owner. Where appropriate labelling shall be in line with the Government Protective Marking Scheme
	4.4 RECOMMEND static ARP and DNS 5.3 RECOMMEND quarterly scan for vulnerabilities 5.4 RECOMMEND configuration checks 7.1 RFC 1918 compliant IP addresses 7.2 Static IP addresses for servers 8.1 EAL4 firewall between organisation and the GSi 8.4 GPS approval for changes to GSi firewall configuration 9.1 – 9.5 IDS 16.3 Refer to GPS for access to other domains via PSI 17.1 Http and smtp via a proxy server – RECOMMEND for IL2, MUST for IL3 17.2 RECOMMEND proxy servers authenticate hosts 17.3 Proxy servers ensure users are authenticated and access controls enforced 20.2 RECOMMEND macro security set to high 21.1 RECOMMEND HTML disabled for email 21.6 Email not auto forwarded outside GSi domain 22.1 – 22.7 Mail server controls. 22.3 no use of GSi email address as a source address by other organisations RECOMMEND for IL2, MUST for IL3		

References

Note	The PSN Universal Reference Sheet provides additional information regarding the products referenced in this document. The Reference Sheet can be found in the Resources and Documentation section of the website. Please note the exceptions listed below.
E3	HMG Information Assurance Standard No. 1, Technical Risk Assessment, Part 1, Issue 3.6, October 2010 (NPM). ^
E3	HMG Information Assurance Standard No. 1, Technical Risk Assessment, Part 2, Issue 3.6, October 2010 (NPM). ^
E3	HMG Information Assurance Standard No. 4, Comsec and Cryptography, Management of Cryptographic Systems, Issue 4.0, October 2009 - (UK RESTRICTED). ^
E3	HMG Information Assurance Standard No. 7, Authentication of Internal Users of ICT Systems Handling Government Information, Issue 1.0, October 2010 (NPM). ^
E5	CESG Good Practice Guide No.10 - Remote Working - Issue 2.0, April 2010 – (UK RESTRICTED). ^
E5	CESG Good Practice Guide No. 13 - Protective Monitoring for HMG ICT Systems, Issue 1.5, August 2010 (NPM). ^

^ Available from - CESG Information Assurance Portfolio website or by contacting enquiries@cesg.gsi.gov.uk. Access can be requested by contacting enquiries@cesg.gsi.gov.uk, it should be known that there might be distribution restrictions