

## Security in the Supply Chain – Guidance Notes

Any person employed by or contracted to Sellafield Ltd is bound by the regulations that govern the UK civil nuclear industry. Security is a priority issue for Sellafield Ltd, and as such the security regulations must be strictly adhered to – this includes security of information in the Supply Chain.

It must be understood from the earliest possible stage by those wishing to tender for sensitive contracts with Sellafield Ltd, that there are security requirements, both at the tender and the placement of contracts stages relating to the protection of information. The requirements differ depending on the classification of the information.

This may involve Government Protectively Marked Information (PMI) - this type of information must be protected in an appropriate way. It may also involve Sellafield Ltd Commercially Marked information, and likewise we would expect that this is protected appropriately, often in a similar way to the Government PMI.

Please take the time to read the following guidance and advice that details the Contractor's responsibility for security in the Supply Chain, and how Sellafield Ltd incorporates this into the procurement process.

### The Regulations

All companies and individuals employed by, contracted to or working in partnership with your organisation with responsibility for any protectively marked aspects will be bound by Section 79 (& 80 if applicable) of the Anti-Terrorism Crime and Security Act 2001 and Regulation 22 of the Nuclear Industries Security Regulations 2003.

\*All PMI held during the Tender process must only be dealt with by companies either with a UK office or by companies located in countries with a bilateral agreement covering the security of protectively marked information.

Anti-Terrorism Crime and Security Act 2001:

[http://www.opsi.gov.uk/acts/acts2001/ukpga\\_20010024\\_en\\_7](http://www.opsi.gov.uk/acts/acts2001/ukpga_20010024_en_7)

- This applies to individuals in the UK and to UK nationals abroad \*see above note.
- All persons in the UK and UK citizens abroad are bound by Section 79 of the above act, entitled: **'Prohibition of Disclosures Relating to Nuclear Security'**
- In basic terms: All those employed by or contracted to your organisation must not disclose, without appropriate authority, any information, **whether or not it bears or attracts a protective marking**, that may be counter to the interests of the United Kingdom or of Sellafield Ltd.
- To do so, either intentionally or recklessly, may constitute a breach of section 79, which may result in prosecution.

Nuclear Industries Security Regulations 2003:

<http://www.opsi.gov.uk/si/si2003/20030403.htm#22>

- Specifically, Regulation 22 of the NISR 2003 is relevant where many contractors are concerned. It details the duties of persons with sensitive nuclear information outside of a nuclear licensed site.

### The 'Need to Know Principle'

Underpinning both of these regulations in the context of information being released into the supply chain is the NEED TO KNOW principle. i.e. not providing more information than is needed to carry out work in a safe, secure and efficient manner.

All Government PMI and Sellafield Ltd COMMERCIAL information should be treated with the 'Need to Know Principle' – it should only be able to be accessed by those people who NEED to see the information to carry out their work.

### **The Protection of Information**

It is the responsibility of Sellafield Ltd to ensure that companies within its supply chain are firstly aware of the regulations and secondly are approved for access to certain types of sensitive information.

Once approved a company is responsible for protection of the information and compliance with the UK legislation listed above. The process by which Sellafield Ltd will enforce this is detailed later in this guidance.

### **Protective Marking of Sensitive Information**

It will be a requirement of the Contractor to comply with all legislation and regulation to maintain the appropriate protection of the information and to ensure that when working with consortium members / partners or sub-contractors, the requirements flow through to these companies.

As a holder of Sellafield Ltd COMMERCIAL or RESTRICTED information, a contractor must assume responsibility for security of their premises/location where the information will be held.

### **Commercial Markings** (See "Mini-Guide Commercial" ref: Infsec-cont-004)

Information may be of a Commercial value to Sellafield Ltd, and documents may contain information of a commercially sensitive nature. Information of this type may be marked with the following headers and footers:- "COMMERCIAL", "AUTHORISED DISTRIBUTION ONLY" or "LISTED READERS ONLY". The requirements include, but are not limited to the following:-

- ❖ Information can only be discussed, copied or otherwise communicated on a "Need to know" principle. No more information than necessary for performance against the scope of work should be supplied. Information can be processed on a company network, IT system or Standalone if the principles of ISO27001 are applied or the Contractor is Accredited to ISO27001.

### **Government Markings**

If documents contain classified information (PMI), the protection and controls are set by UK Government it is the responsibility of Sellafield Ltd to ensure that companies within its supply chain are firstly aware of the regulations and secondly are approved/authorised where appropriate.

Government Protective Markings (RESTRICTED, CONFIDENTIAL, SECRET and TOP SECRET) may apply to contracts that are being let by Sellafield Ltd, as well as the documentation that is released at the Invitation to Tender Stage. Sellafield Ltd contracts and tender documentation may also be marked with a company classification at a Commercial level instead of or as well as a Government protective marking.

The requirements for Contractors to be able to process information of that nature include, but are not limited to the following:

### **RESTRICTED PMI** (See "Mini-Guide RESTRICTED" ref: Infsec-cont-005)

- ❖ "Need to know" principle as above.
- ❖ No formal clearance required however companies are responsible for carrying out a formal ID, nationality and right to work check.
- ❖ Approval of the location by Sellafield Ltd for holding RESTRICTED information or
- ❖ List X approval by the MOD or AWE and working to the Security Policy Framework at all addresses where the RESTRICTED PMI will be held or
- ❖ Approval for CONFIDENTIAL (List N) by The Office for Civil Nuclear Security and working to the Manual of Protective Security and Civil Nuclear Security Supplements at all addresses where the RESTRICTED PMI will be held.
- ❖ Signature and return of a Security Aspects Letter.

- ❖ Advanced notification to, and the approval of Sellafield Ltd prior to any PMI being handled at locations to allow for verification checks / assessments to be made where applicable.
- ❖ For the processing of RESTRICTED PMI on a small local network or IT systems, including stand alone PCs, to implement the HMG standards for Accreditation and to be formally Accredited either by:-
  - a) Sellafield Ltd being provided with a Risk Management Accreditation Document Set for assessment and Approval
  - b) via MOD, AWE or OCNS with a signed Risk Management Accreditation Document Set as evidence provided or
  - c) Processed on the Sellafield Ltd network.

Note: Self accredited RESTRICTED networks used by some List X companies are not recognised by the Office for Civil Nuclear Security and must not be used.

Note: For the Accreditation process a Security representative from within the Contractor must have attended the National School of Government Training or request the use of a CLAS (CESG Listed Adviser Scheme) Consultant [http://www.cesg.gov.uk/products\\_services/iacs/clas/index.shtml](http://www.cesg.gov.uk/products_services/iacs/clas/index.shtml)

**CONFIDENTIAL PMI** (See "Mini-Guide CONFIDENTIAL" ref: Infsec-cont-006)

- ❖ "Need to know" principle as above.
- ❖ Staff cleared to "Baseline Personal Security Standard".
- ❖ List X approval by the MOD or AWE and working to the Security Policy Framework at all addresses where the CONFIDENTIAL PMI will be held or
- ❖ Approval for CONFIDENTIAL (List N) by The Office for Civil Nuclear Security and working to the Manual of Protective Security and Civil Nuclear Security Supplements at all addresses where the CONFIDENTIAL PMI will be held.
- ❖ Signature and return of a Security Aspects Letter.
- ❖ For the processing of CONFIDENTIAL PMI, a small local network (with No Internet connection) or Standalone system accredited by MOD, AWE or OCNS with evidence provided.

## **The Sellafield Ltd Process – Supply Chain Security**

### **Invitation to Tender**

Sellafield Ltd will assess suitability of each location, on the basis of declarations made by the company for each location where sensitive information will be kept and/or processed. For contracts that are at the Invitation to Tender stage, Sellafield Ltd will ask for each tendering company to complete a security Declaration, which is an agreement that the tendering company will abide by certain rules regarding the protection of sensitive information. (See: "Security Declaration and Risk Assessment – Invitation to Tender" ref: Infsec-cont-002)

The tendering company will be required to provide their current security policies and procedures that as a minimum cover the basic requirements specified in the Declaration.

NOTE: This also applies to all sub-contractors, consortium members etc, and it is the responsibility of the lead tendering company to disseminate the Declaration requirement to them.

Sellafield Ltd will issue a Tender Authorisation Certificate, as an acceptance that the security of the location has been declared to meet the minimum requirements for the security of hard-copy (paper) RESTRICTED information for the purposes of Invitations to Tender. The Tender Authorisation Certificate is valid for a 12 month period and can be referenced in other Sellafield Invitations to Tender during that period. However, no PMI will be sent to the company until a signed Security Aspects Letter has been received by Sellafield Ltd (See below).

After signing and returning the declaration a company may be subject to Security Assessments at short notice to be carried out either by Sellafield Ltd or Inspectors from the Office for Civil Nuclear Security.

### **Contract Award Stage**

When a contract is awarded that involves PMI, the Contractor will be subjected to a full security assessment at each location where the information will be held/processed before the contract can commence.

Sellafield Ltd's Security Department will visit each location/premises where PMI will be held / processed and complete their assessment, based upon criteria set by the security regulator, OCNS.

If the criteria are met, Sellafield Ltd will issue a Certificate of Approval for holding hard-copy (paper) RESTRICTED PMI. This will be valid for 3 years (conditional) and will replace the Tender Authorisation Certificate. The Certificate of Approval can be referenced in future tenders.

### **Security Aspects Letters**

At Invitation to Tender each company will be issued with a Security Aspects Letter. This will require a signature, which confirms that those involved with that particular Tender fully understand what types of information they are able to process and those they are not. It contains details of the aspects of the documentation that will attract a protective or commercial marking and includes a reminder of security obligations under the Nuclear Industries Security Regulations 2003 and the Anti-Terrorism, Crime and Security Act 2001.

No PMI may be issued until the Letter is signed and returned to Sellafield Ltd.

The Tender Stage Aspects Letter will contain slightly less detail, as the documentation released to the tendering company will already be marked when it is issued out. No PMI should have to be produced by the tendering company at this stage. The guidance contained within the Aspects Letter will help to avoid doing so. (COMMERCIAL information may be produced).

At the Contract Award Stage a further Security Aspects Letter will need to be signed. This will reflect the full aspects of the contracted scope of work and will cover the electronic processing / storage of PMI (if applicable). The guidance contained within the aspects letter should help ascertain the correct marking of any documentation produced and how to avoid going higher than the approval will allow.

### **Access to Information**

Once the Security Aspects Letter (At both Invitation to Tender and Contract Award stages) has been signed and returned, the relevant PMI may be issued.

RESTRICTED level information will be issued in hard-copy only, via post or fax (at Contract Award stage this may be done, subject to controls, using electronic / optical removable media where the Accreditation requirements of the receiving system have been met).

If CONFIDENTIAL level information is required at the Invitation to Tender stage the tendering company/contractor will be invited to a Sellafield Ltd location in order to view the information.

### **Changes to Security Measures**

The Tender Authorisation Certificate and the Certificate of Approval only reflect the state of security at a location at a specific time.

As such, Sellafield Ltd Security Department should be informed if any changes are made to a premises that may directly, or indirectly, affect the level of security that was present at the time of authorisation.

A few examples of circumstances are:

- If the company changes its name, or is sold to another entity
- If the location of the PMI is changed
- If physical changes are made to the premises that may compromise security
- If the Security Controller/Security Contact changes
- If the security procedures relating to the protection of the PMI change\*
- If the security policy is changed\*
- If the company Board of Directors/Executive is changed

\*In these instances, copies of the revised versions of the procedure and/or policy should be sent to Sellafield Ltd Security Department for retention on file.

This is not an exhaustive list, therefore if there are any issues which may be thought to affect security at the premises, the Security Department should be contacted.

Once a Declaration has been signed, the tendering company / contractor will be bound to certain security obligations, including:

- Application of the 'Need to Know' Principle.
- Producing and maintaining security policy and procedures .
- Not employing sub-contractors to work on Sellafield Ltd contracts at locations other than the declared location without prior notification to Sellafield Ltd Security Department.
- Appropriate controls of access to PMI and COMMERCIAL information .
- Return of or written assurance of the destruction and all PMI and COMMERCIAL information at the end of the Invitation to Tender process and/or the completion of the contract.

The correct application of all of the above points should ensure that section 79 of the Anti-Terrorism, Crime & Security Act 2001 is not breached.