SECURITY POLICY IN A COMPLEX LOGISTICS PROCUREMENT[1]

Michael J. Nash* and Wing Commander Ronald J. Kennett RAF**

***Gamma Secure Systems Limited**
Diamond House, 149 Frimley Road, Camberley, Surrey, GU15 2PS, United Kingdom

****Ministry of Defence**
Penderel House, High Holborn, London WC1V 7HX, United Kingdom

ABSTRACT

The Royal Air Force Logistics Information Technology System (LITS) is a ten year United Kingdom procurement programme to provide the Royal Air Force with a fully integrated IT system covering its Supply and Engineering functions. It will hold and process classified information and thus requires an IT security policy. Although a single integrated system, it will service many distinct locations and types of applications, and will be developed and put into operational use over this extended period. It will also link to many related logistics and other support systems. It has been found necessary to define a hierarchy of security policies covering the full scope and extent of the system, and it may be necessary to have multiple security targets for security evaluation.

BACKGROUND

The United Kingdom Royal Air Force (RAF) has always been a leading user of Information Technology (IT) and has used IT in its supply functions since 1966. However, its systems have tended to be planned and developed in isolation, with insufficient regard for the real needs of users, and with overlaps and incompatibilities between systems. In the mid 1980s, the Ministry of Defence (MOD) recognised that similar deficiencies existed throughout all the UK armed services and its MOD support organisation, the Procurement Executive (PE). It was therefore decided that these four main elements of the MOD (the Royal Navy, the Army, the Royal Air Force and the Procurement Executive) would each undertake a series of strategic IT studies, in the three key functional areas of logistics, personnel, and command and management. The RAF started its logistics strategy study in 1988. Its aim was to define the IT strategy required to support the logistics objectives of the RAF into the 1990s and beyond. The principal objectives were to define the target IT systems required, to specify a plan for migration from the existing systems to the target systems, to determine the organisation required to manage and control the migration, and to specify the management activities required to implement the strategy.

The RAF logistics strategy study was completed in 1989. It indicated that by initiating a ten year programme to provide the RAF logistics community with a fully integrated IT system covering its supply and engineering organisation, an IT development costing about £500M (approximately $750M), would result in savings to the RAF of over £1000M (approximately $1500M).

As well as identifying potential cost savings, the study also revealed that in many areas the current planning, management and control of RAF logistics functions were manpower intensive and imprecise. There was a serious lack of information about logistics activities and their associated costs for use in policy formation and review. The existing logistics systems had largely been designed to meet operational needs of discrete groups of users and were not designed to share common data or provide aggregated management information. The major RAF central logistics systems employed ageing technology and used inconsistent technical and data standards. More importantly, they did not meet the

---

[1] PUBLISHED AT THE NINTH ANNUAL COMPUTER SECURITY APPLICATIONS CONFERENCE, ORLANDO, FLORIDA, 6-10 DECEMBER 1993. (pp. 46-53)

users' current needs. Overall, it concluded that the existing systems did not provide an adequate basis to meet anticipated future service demands - and did not provide a sound basis for piecemeal future developments. Thus it was necessary to start again from scratch, building a new and comprehensive logistics system covering all aspects of supply and engineering in an integrated manner.

A final complication was that no new funding for IT development was to be made available. Thus the programme had to be financed entirely from savings in logistics costs. This meant that there would be great pressure during the programme to avoid delays and cost overruns, and to show actual benefits as early in the life of the programme as possible. Indeed, it was decided that certain key areas should receive new "fast track" IT systems, where the investment analysis indicated high short-term returns from early investment were possible. However, it was accepted that integrating these "fast track" systems into the full LITS system at a later date might be difficult.

The LITS strategy study identified that the new system would inevitably have to process classified information, and thus security would need to be addressed throughout the programme, from its outset.

THE UK SECURITY REQUIREMENT

Any IT system in the UK which is used to process classified information must possess a System Security Policy (SSP) and be formally security accredited before entering live operation - this applies not only to Government systems, but also those in Industry. Accreditation is a formal confirmation by the appropriate Departmental Security Officer that adequate security measures have been put in place and that use of the System in accordance with its SSP does not present an unacceptable risk to national security.

The Communications-Electronics Security Group (CESG) of the UK Government Communications Headquarters (GCHQ) is the UK Authority responsible for providing guidance on IT security for protecting national security. As such, it is one of the key UK contributors to the European Community ITSEC/ITSEM initiatives [1, 2]. It publishes and distributes, on a controlled basis, a wide range of Infosec handbooks covering most aspects of IT security. Amongst these handbooks is one specifically aimed at writing Security Policies for IT systems [3]. Others cover related issues, such as security within the project lifecycle [4].

The SSP, and the Accreditation for live operation which is based upon it, take into account the overall security of the system. CESG guidance [3] suggests that the SSP should define the environment within which the system will operate and the protective measures which are to be applied. The SSP should include sections on access control, authentication, accountability, audit, object reuse, Comsec, integrity, availability and security administration. For each section, the environmental measures that are needed to provide the required level of protection should be documented (many of these will be standard to all Government sites), together with the security requirements to be implemented in the system.

Overall security is thus achieved using a combination of technical and non-technical security measures, which may be interrelated. Where the SSP calls for technical security measures to be enforced by the system (as distinct from those enforced by physical, procedural or personnel measures in the surrounding environment), the Accreditor may call for security evaluation, followed by certification by the UK IT Security Certification Body (CB). The CB is a Government organisation, jointly run by CESG and the UK Department of Trade and Industry, but functionally independent of both. Certification in this sense is a formal statement of the extent to which the security functions implemented in hardware, firmware and software meet the stated technical security requirements. In the UK, this is based on the results of an independent computer security evaluation, conducted by a Commercial Licensed Evaluation Facility (CLEF) according to standards and procedures mandated by the CB, and paid for by the system sponsor or developer [5].

One of CESG's handbooks recommends minimum functionality requirements for various system operating modes, and minimum assurance evaluation levels, dependent upon key system characteristics [6]. Within the RAF, similar but more specific guidance exists, also made available on a controlled basis [7]. These recommendations are, of course, not system specific, and Accreditors may demand higher or accept lower minimum standards for particular systems, depending on individual system circumstances.

The security evaluation and certification process within the UK applies equally to IT systems and IT products. The CB will issue certificates both to developers of security products, who wish to use the certificate for marketing purposes, and also to system developers who need to demonstrate to an Accreditor that use of the system will not present a risk to security. The same technical standards and procedures are used in both types of evaluation, although product evaluations are based on a generic security target, specifying assumed threats and an assumed environment, whereas system evaluations are more specific and the target defines stated threats and the actual environment.

This contrasts to the US approach, where product evaluation and certification is performed by NCSC against the TCSEC criteria [8], but system evaluation and certification, although mandatory under OMB Circular A-130, is a more informal and non-uniform process, very much at the discretion of the procuring agency [9, Appendix B].

THE LITS PROCUREMENT ORGANISATION

The RAF Directorate of Logistics Information Systems (DLIS(RAF)), was set up in 1989 to manage the development of the LITS programme and to take over management of current RAF logistics IT systems until they were subsumed by or integrated into LITS. Because of the size and integrated nature of the proposed new LITS system, IT security was seen as a major potential risk to the programme, which would need to be managed on a full-time basis: this was a new idea for the RAF at the time. In consequence, a full time service post was established at Squadron Leader (Major) level to take on responsibility for the area.

A year into the project, the importance of IT security had been confirmed by practical experience, and the value of the service post had easily been demonstrated. However, it was also clear that the responsibilities of the post were greater than originally envisaged, and it was therefore deemed essential to raise the level of the post from Squadron Leader to Wing Commander (Lieutenant Colonel). Hindsight shows this decision to have been correct, and to have been taken just in sufficient time for liaison links to other security organisations and parts of the RAF to be set up at the right level.

The Wing Commander is responsible for setting the IT Security Policy for the LITS programme, within the general guidelines set out by the RAF security authorities. It was also decided that the incumbent for the post should have a RAF logistics background, since at the project development level it would be important to understand the implications of the policy being developed. IT experience and appropriate IT security training were also thought to be essential. All of these criteria have been found to be fully justified in practice. The Wing Commander is supported by experienced IT security consultants contracted from industry. One consultant post specifically advises on strategic security issues, others perform security studies and monitor the work of the development contractors for the programme. This combination of RAF experience and industry expertise has resulted in a strong DLIS(RAF) IT Security Policy Branch, where we are able to maintain effective control over IT security within the programme.

Like all UK projects proposing to process classified information, we can call on CESG for advice and guidance, through its User Liaison Branch. Because of its strategic, long term nature, we in LITS are additionally supported with technical advice from within CESG. Furthermore, we are supported by a Security Working Group that meets regularly, at which CESG, the RAF Comsec Authority and the LITS Accreditor are represented.

The RAF security organisation is the RAF Directorate of Security. IT security accreditation for the RAF is performed by the IT Security Branch of this organisation. However, the scope of LITS extends beyond the RAF, with terminals planned to be located on sites and buildings belonging to the two other UK armed services and the UK Ministry of Defence Procurement Executive. Each of these has its own accreditation agency. One of the early decisions taken by the LITS Security Policy Branch was to ask for a single point of contact for accreditation to be nominated. The various accreditation agencies readily agreed to this, and nominated the RAF Accreditor to be the Lead Accreditor. The RAF Accreditor chairs an accreditation panel made up of all the accreditation agencies, and acts as the point of contact and decision authority for the panel. We have found that this has greatly simplified and speeded our approval process for policy documents.

THE LITS PROCUREMENT STRATEGY

It was decided very early in the LITS programme that the size and duration of the proposed IT development required that the work was managed as three separate major sub-projects, called tranches. Each tranche would cover specific application areas. Furthermore, each tranche would also be split into two parts for contract purposes, a Full Study Contract, and a Development Contract. The Full Study Contract would cover requirements definition and analysis, and the Development Contract design, development and implementation. The two contracts for each tranche would be mutually exclusive, with any contractor winning a full study being disbared from competing for the associated development contract. It was also decided that the winning contractor for development of the first Tranche would also act as the Prime Systems Integrator, responsible for integration of the work of the other development contractors for the other tranches into the evolving LITS system.

The UK Government has a preferred systems study method called SSADM (Structured System Analysis and Development Methodology), and it was decided to impose it on the LITS programme. The UK Government also has a preferred methodology for managing projects called PRINCE (Projects in a Controlled Environment), and it was decided to use PRINCE within the DLIS(RAF) Programme Management Team, although not to impose it upon the contractors, so long as their own procedures could interface to the RAF's PRINCE organisation and requirements. Neither methodology is ideally suited for handling IT security requirements, particularly where evaluation and certification is required, and it was necessary for us in the DLIS(RAF) Security Policy Branch to devise our own modifications for use handling the IT security aspects of the programme [10].

A further complication for LITS programme management was its wide geographic coverage (there will be LITS terminals in some 80 sites in at least 12 countries). It therefore appeared impractical for the whole of each LITS tranche to be put live concurrently. Instead, it was envisaged that each LITS tranche would be introduced into live operation gradually, adding new applications or coverage for additional types of aircraft, in an incremental approach: this has subsequently been confirmed as essential by the formal Tranche 1 Full Study requirements analysis. Before the first fielding of any part of LITS, security accreditation would be required. This accreditation would then need to be re-assessed and updated throughout the life of the programme as further LITS coverage and applications were rolled out.

SYSTEM SECURITY POLICIES

CESG's guidance is that every system that processes classified information must have an SSP. The SSP goes through various stages of refinement, from an SSP (Initial), which merely identifies key facts about the system, to an SSP (Final), produced following user acceptance trials and matching the actual operational system. This approach, shown in Figure 1, is mandated by the RAF Accreditation Branch on all RAF systems. Where a system places significant reliance on security measures implemented in software or hardware, CESG recommends that the technical measures are separated from the environmental measures, and documented in a System Electronic Information Security Policy (SEISP).

The SEISP also documents the security architecture of the system, so that the electronic measures can be placed into an overall system context (that is, the SSP says “what” and the SEISP “how”).

Although it is up to the Accreditor of a system to decide when IT security certification by the CB is required, it is likely to correspond to those systems placing reliance on technical IT security measures and thus requiring a separate SEISP. The SEISP and associated SSP become the security target for evaluation by a CLEF. The SEISP defines the required security functionality, the SSP documents the environment surrounding the system.

In these days of interworking between systems, many classified systems exchange data and perhaps provide processing facilities to users of other systems: LITS will be no exception. In the longer term, LITS will almost certainly be electronically linked to the logistics systems of all the other UK armed services and, through Electronic Data Interchange (EDI), to the support and accounting systems of its suppliers. To achieve the maximum benefits of integration, it will be necessary for LITS to place at least some reliance in the security measures of the other systems to which it is linked, and vice versa. In such cases CESG recommends that a System Interconnection Security Policy (SISP) is defined for each interconnection, to document the security risks presented by the interconnection, and the agreed

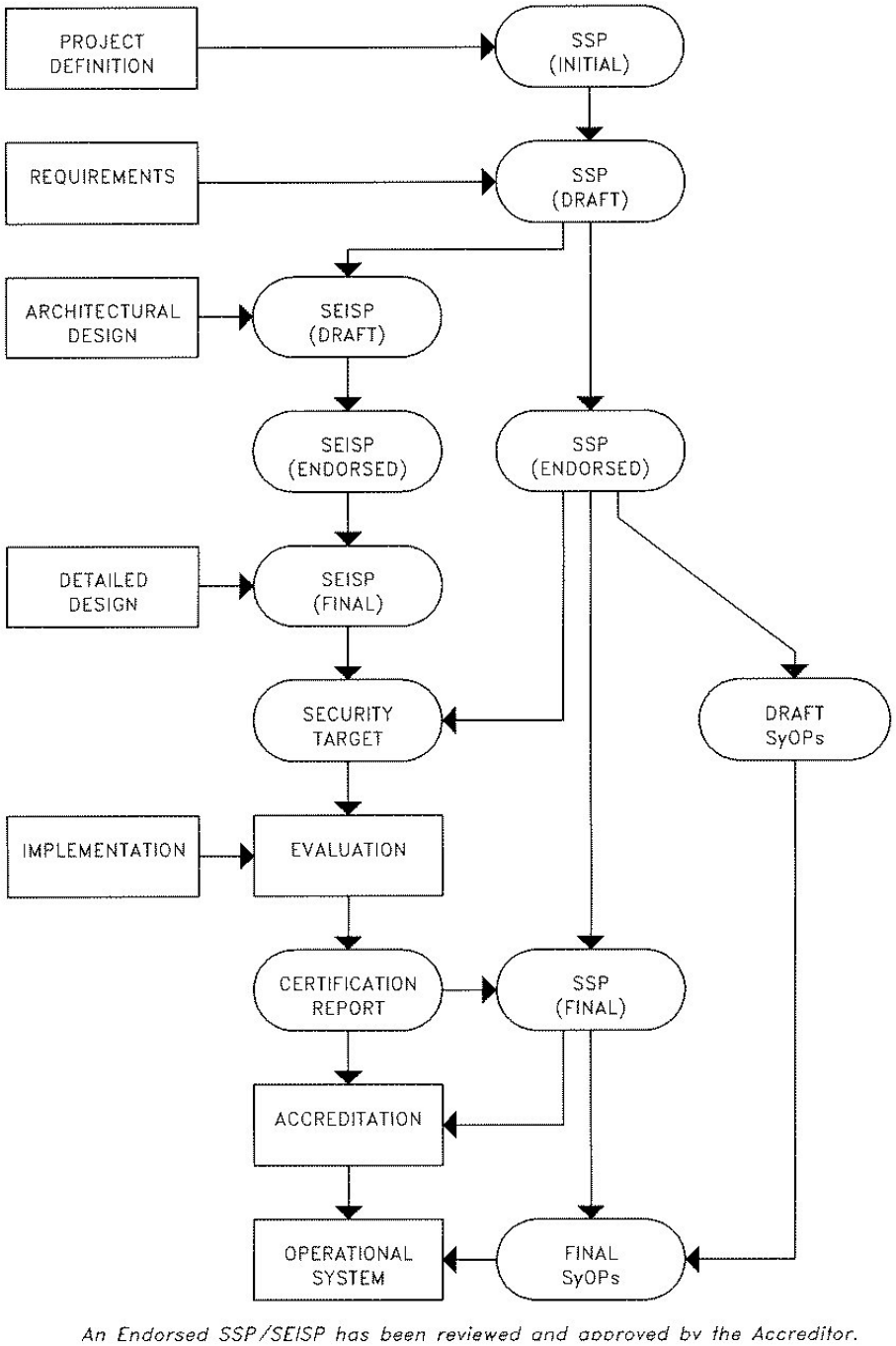

Figure 1 - CESG Guidance

security measures to be provided by both parties to counter those risks. Where several secure systems interwork as part of a network community, CESG suggests that it is best to have a standardised approach, imposed on all interconnections between community members. The common "standard protection" security measures to be provided by all members are recorded in a single Community Security Policy (CSP). The CSP also identifies the member systems and all their interconnections. It enables the individual SISPs for each interconnection to be reduced in size and simplified to recording only exceptional measures.

THE INITIAL LITS PROGRAMME APPROACH

Once the LITS Security Policy Branch had been established, our first major task was to produce an initial version of an SSP, following the CESG guidelines for SSP structure. We quickly realised that some of the detailed information that would be necessary in a full SSP could only be established later in the programme, following proper requirements analysis work. We therefore decided to call the high-level document that we were producing the "Programme Security Policy", or PSP for short (of course, written in UK English, this cannot be confused with a security policy for a single computer program!). The PSP was intended to be an overarching policy for the whole ten year logistics strategy, concentrating on programme security objectives, but also mandating security measures in detail where we thought that they would be appropriate throughout the whole of the LITS system. We tried to include as much explanatory information as possible, so that the study contractors could follow the reasoning behind our choice of measures. It was our intention to have the PSP approved by the Accreditor before the Tranche 1 Full Study began. The PSP would then be refined by the study contractor into a full LITS SSP, as one task within the overall requirements analysis work.

Producing the PSP generated a list of major security issues that we judged would be directly relevant to LITS, but where we could find no applicable guidance in the documentation available from the RAF Security Branch or from CESG. Some of these resulted from sections of the CESG recommended SSP structure where we had no idea what to put in the context of a long-term, integrated system. Following discussions with the RAF Accreditor and our CESG support, we realised that there were no easy answers to most of these issues: in many areas we were breaking new ground due to the size and complexity of the LITS system and the chosen procurement approach.

However, before the Tranche 1 Study Contractor was appointed, the RAF Accreditor sent us a first draft of a proposed RAF Functional Areas Community Security Policy for comment. This had been prepared by the strategy study team for one of the other RAF key functional areas, and was intended to cover interworking between all RAF systems in the logistics, personnel, and command and management areas. It was clear to us that interworking between LITS and systems within the two other RAF functional areas would be important - and would be complicated by the fact that the other two functional areas intended to follow evolutionary and less tightly integrated approaches towards new IT systems development.

The draft CSP went into great detail in specifying mandatory security measures to be incorporated in all systems, and placed great emphasis on developing new RAF security standards. For example, it placed minimum requirements on all data entry devices that would have prohibited the use of bar code readers. Many of the mandated measures seemed to be unrelated to interworking. We gave the draft CSP careful consideration, and reluctantly decided that we could not support its introduction as community policy. Our formal objection was that the document failed to identify the community security objectives it was trying to implement. When we posited likely objectives, the document failed to meet them. We suggested that the CSP needed radical modification, to become a much more high level document, dealing exclusively with interworking between systems, and setting minimum requirements linked clearly to interworking security objectives and threats.

We made our reservations known to the RAF Accreditor, and the staffs of the other functional areas. Unfortunately, everyone agreed with us. The RAF Accreditor therefore tasked us with rewriting the CSP. We produced a new and substantially shorter proposal, dealing exclusively with community interworking. Subsequently it has been endorsed by all three functional areas and the RAF Accreditor, and formally issued as the RAF Functional Areas Information Systems Community Security Policy.

The development of this CSP rather changed our views of the value of the PSP we were developing for LITS. It became clear that some of the criticisms we had levelled at the original draft CSP could equally well be made about the LITS PSP. There was no justification, prior to the results of the full studies, to mandate detailed security measures on all parts of the LITS system. We therefore came to the conclusion that LITS might require a number of SSPs, prepared at different times and covering individual areas within the programme as they were formally analysed, specified and implemented. These SSPs could contain different security measures, depending on differences in requirements, selected technology and system location (for example, UK or overseas).

However, there was still a need to set a security policy framework for the programme. We still needed a way to specify a set of identified risks and threats to security to be considered by the study contractors. These would scope the security requirements analysis of each part of LITS, in each case generating detailed security measures to be incorporated within that part. We therefore revised the PSP to reflect this new approach, producing a document that concentrated on identifying security risk factors and threats common to all parts of LITS.

We had a further problem at programme level. Our proposed approach to security had to be consistent with SSADM's lifecycle development model. This meant we could not formally determine the assurance requirements for LITS until the Tranche 1 Development Contractor was appointed, since the technical architecture was to be specified by the development contractor. However, we needed assurance and functionality targets immediately, in order to confirm programme feasibility and the viability of financial budgets. We therefore developed a "reference" high-level security architecture, representing one way of implementing LITS with currently available IT technology. This gave us sufficient information to apply the algorithms in [7]. Using our reference architecture, we showed that LITS could be implemented as two networks of linked system high systems, running at Restricted and Secret respectively. (Restricted is a UK hierarchical security classification level, between Unclassified and Confidential). The systems forming these networks needed ITSEC E2 or E3 assurance, and F-C2 functionality. There was a need for a limited number of higher assurance Guards to pass information between the Restricted and Secret networks. These needed E4 or E5 assurance, and specialist one-way regulator functionality.

This reference architecture was incorporated in the PSP as an appendix. It was not to be imposed on the LITS contractors; they were free to choose any security architecture they wanted. However, it gave us confidence that our programme security objectives were not unrealistic. Our proposed PSP, revised as described above, was reviewed by the RAF Accreditor and our CESG support, and then issued as a LITS policy document to the Tranche 1 Full Study Contractor, when he was appointed.

THE LITS TRANCHE 1 SECURITY APPROACH

Following a competitive tendering process, CSC Europe was chosen as the Tranche 1 Full Study Contractor. Following the DLIS(RAF) security policy set out in the CSP and PSP, and based on extensive security requirements analysis, they successfully produced an SSP for LITS Tranche 1, which is now at SSP (Endorsed) status. One innovation that CSC found necessary was the extensive use of italics in the SSP to pass advisory information to the Tranche 1 Development Contractor, when appointed. This information identifies unresolved issues, and explains some non-intuitive decisions and requirements. The development contractor will have to act on this additional information, removing it from the document before it is issued as the SSP (Final).

CSC was also contracted to produce a contribution to a Tranche 1 SEISP, and a number of outline SISPs to other non-LITS systems. In retrospect, these deliverables were premature. Without known technical and security architectures, both of which would be development contractor responsibilities to define, these documents were too theoretical to be of great use to the Programme. However, they did expose some additional security issues and enable us to incorporate them within the Tranche 1 Development Contractor's stated scope of work.

CSC also was to produce a number of security working papers. One of these examined real potential security architectures. We were able to use the concrete information in this working paper as the basis for target functionality and assurance levels, superseding the theoretical reference security architecture in the PSP. In turn, this enabled us to remove the reference architecture from the PSP version issued to potential development contractors. This made the PSP completely architecture and technology independent, as is appropriate for a programme level policy document. We were also able to add to the PSP some additional factual information on data volumes and classifications etc., as established by the first study.

Finally, the CSC study confirmed the need for both application and location roll out during LITS Tranche 1 development. This means that multiple security accreditations will inevitably be required, and in consequence there will most likely need to be multiple security targets for evaluation. The Tranche 1 Development Contractor may well wish to have several different SEISPs, covering either

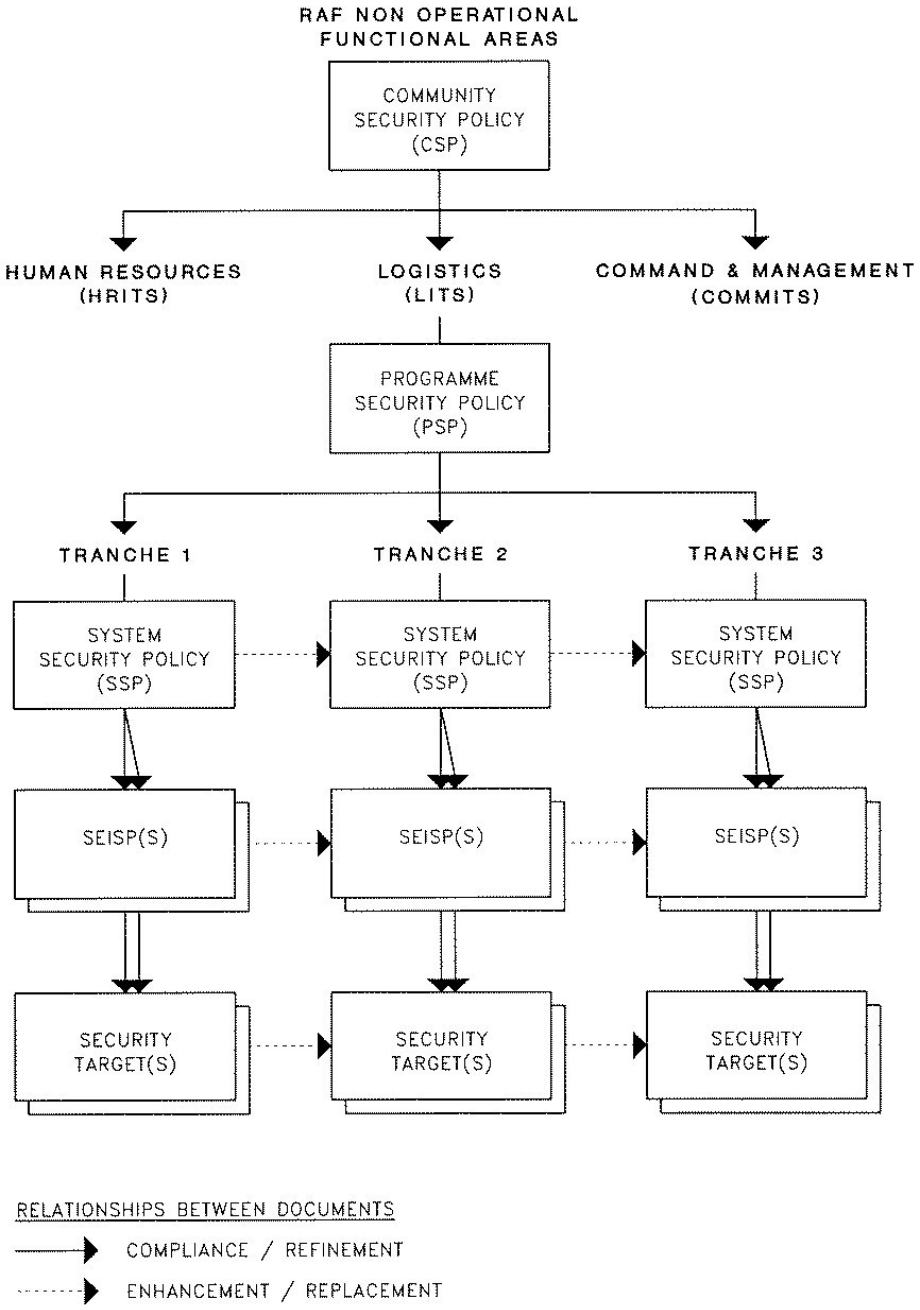

Figure 2 - Relationships

different types of installation, or reflecting phased implementation of security functionality as larger or more sensitive applications are added to the initial fielding.

Because of the need for Tranche 1 roll out, it is likely that the Tranche 1 Development Contractor will choose to have a series of security targets for evaluation. These need not be specific to particular sites: differences between sites in their local environments can be covered in site specific Security Operating Procedures (SyOPs), provided that the dependencies are adequately documented in the associated security target. If the development contractor employs a single CLEF, there is no reason why evaluation results for one security target cannot be directly reused for a later target if the evaluated functionality is unchanged.

The relationships between all these actual and possible security policy and evaluation target documents are shown in Figure 2.

FUTURE ACTIVITIES

CSC's contract has now been extended to cover the Full Study for LITS Tranche 2. We have asked them to develop an SSP for Tranche 2, either as a separate policy document or as a single revised Tranche 1 SSP, updated to cover both Tranches. Since development work on the implementation of Tranche 1 will be proceeding in parallel, it would be contractually simpler to have two separate documents, but it is not clear without a proper analysis to identify the differences between Tranche 1 and Tranche 2 security requirements that this is the best technical approach.

We are in the process of selecting the Tranche 1 Development Contractor. As he will also act as the future Prime Systems Integrator, this is a key appointment: we anticipate that the selection process from original advertisement in the EC Journal will take nearly two years. As part of the selection process, companies and consortia selected to respond to the Operational Requirement will be required to put forward a proposed technical architecture, including a security architecture. The successful bidder's proposed security architecture will be used, in conjunction with the Tranche 1 SSP, as the foundation for the development of the Tranche 1 SEISP or SEISPs. These SEISPs must not only form a sound basis for security implementation, they must be endorsed as acceptable by the RAF Accreditor. Thus the viability of the proposed security architecture represents a potential prime risk to the success of the Programme. We have therefore decided that companies on the final shortlist will be paid to develop production quality SEISPs from the Tranche 1 SSP and their proposed architecture, before a decision is made on development contract award: similar system procurement studies are planned for other key, non-security, areas.

CONCLUSIONS

LITS has been the first major UK defence functional area to address the IT security aspects of major systems development within the budgetary constraints of paying for IT investment by withdrawal from user operational budgets. This has lead to remarkable user support to minimise the costs of IT security and to headline its potential problems. It has forced us to set realistic and achievable IT security objectives, and to define a clear IT security definition and implementation approach. There is no money in the LITS budget to pay for LITS-specific research or development activities.

We have received strong and positive support from both the RAF security organisation and CESG. We have, however, found that the published CESG IT security handbooks and other guidelines are aimed at the major audience for Government IT security, namely small to middle range systems, implemented in-house as single deployments. We have found that, without thought and modification, many aspects of the CESG guidelines are inappropriate for a long term programme such as LITS.

Within the DLIS(RAF) Security Policy Branch, we have needed to follow a systematic approach to setting and controlling IT security policy. At times we have had to break new theoretical ground in the structuring of policy documents in order to meet the security objectives of the Programme. Our approach has influenced other MOD projects, and in some cases has found its way into official CESG guidance.

LITS has now successfully completed the Full Study for the first of its three tranches of applications. We are in the process of selecting the development contractor for Tranche 1, whilst the Tranche 2 Full Study is already under way in parallel. Our approach to specifying security policy through a hierarchy of IT security policies has been a pragmatic solution to the problems of developing security policy within a complex system procurement approach. It has shown itself to be a very successful solution to the difficulties associated with "problem ownership" during a large and complex development process.

REFERENCES

[1] Information Technology Security Evaluation Criteria, ISBN 92-826-3004-8
Commission of the European Communities, Luxembourg, Version 1.2, June 1991.

[2] Information Technology Security Evaluation Manual
Commission of the European Communities, Luxembourg, Draft Version 0.2, April 1992.

[3] System Security Policies, CESG Infosec Memorandum No. 5
Communications-Electronics Security Group, Cheltenham, UK, Issue 2.0, February 1993.

[4] Security Activities in the Project Life Cycle, CESG Compusec Memorandum No. 11
Communications-Electronics Security Group, Cheltenham, UK, Issue 1.0, March 1991.

[5] Description of Scheme, UKSP01
UK IT Security Evaluation and Certification Scheme, Cheltenham, UK, Issue 1.0, March 1991.

[6] HMG Minimum Computer Security Standards, CESG Compusec Memorandum No. 10
Communications-Electronics Security Group, Cheltenham, UK, Issue 1.0, March 1991.

[7] RAF Manual of Security - Computer Security, AP3086 Supplement 1
Ministry of Defence, London, UK, First Edition, 1993.

[8] Trusted Computer Systems Evaluation Criteria, DOD 5200.28-STD
Department of Defense, USA, December 1985.

[9] Computer Security Considerations in Federal Procurements, NIST Special Publication 800-4
Barbara Guttman, National Institute of Standards and Technology, USA, March 1992.

[10] Information Security In a Complex Defence System Procurement
R. J. Kennett and M. J. Nash, Proceedings of the Fifth Canadian Computer Security Symposium, Ottawa, 1993.