MANAGING INFORMATION SECURITY IN LARGE DEFENCE PROCUREMENTS: THE ROYAL AIR FORCE LITS EXPERIENCE[1]

Wing Commander R J Kennett RAF* and Dr. M J Nash**

***DLIS-LITS Project**
c/o IBM UK Ltd, Stevenage, Hertfordshire SG1 2BJ, United Kingdom

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

ABSTRACT

This paper describes the practical experiences of the authors subsequent to the 1993 Symposium and overlays the procurement process that took place for the development of the first tranche of the Royal Air Force's Logistics Information Technology System from a COMPUSEC perspective. It explains some of the problems encountered by the Security Team during the selection of a Prime Systems Integrator and developer and then describes what actions were taken to minimize the associated security risks. It is believed that many of these management problems and difficulties we have faced and resolved hold equally true for all secure IT system developments. Many of the lessons we have learned are relevant to the management of all secure system procurements where a contractor is used, irrespective of size.

INTRODUCTION

The Royal Air Force (RAF) is undertaking a five hundred million pounds sterling (in excess of one thousand million Canadian dollars), ten year Information Technology (IT) development to update its world-wide engineering and supply systems into one fully integrated logistics system. The strategic aim is to achieve a reduction in support costs of existing and planned weapon systems without prejudice to standards and required levels of availability and sustainability. Under the UK Ministry of Defence's (MOD) financial strategy of delegated budgets to functional areas, identified future cost savings are being used to finance this investment in Information Technology and the logistics budget has been cut accordingly.

A paper was presented to the 5th Annual Canadian Computer Security Symposium in 1993, by the current authors [1]. That paper described some of the IT security problems that they encountered and overcame during the early development stages of the new Royal Air Force Logistics Information Technology Strategy (LITS). It included descriptions of the additional management tasks found necessary to support IT security during the development of this large and complex system. In order to follow the latest HMG advice on IT security, it was necessary to impose changes to the standard UK Government system analysis and project management methodologies.

Since the publication of the previous paper, the project has progressed into the implementation stage. System development of the first tranche of applications is underway. Requirements analysis for the whole of the LITS programme has been completed. A Prime Systems Integrator (PSI) has been selected and appointed to develop and install the IT infrastructure of the programme, and manage the implementation of the LITS application functionality.

---

[1] PUBLISHED AT THE SEVENTH ANNUAL CANADIAN COMPUTER SECURITY SYMPOSIUM, OTTAWA, CANADA, 16-19 MAY 1995. (pp. 129-146)

LITS CONTRACT STRATEGY

The LITS contract strategy was to divide the LITS implementation into 2 main contractual areas; study contracts for each of 3 tranches, and a systems integration contract which also covered the actual development task. The procurement cycle started in 1991 with the issue of a Statement of Programme Requirement which provided an update of the original strategy study undertaken in 1989 and 1990. At that stage approximately 110 companies expressed an interest in taking part in the LITS development. These companies varied dramatically in size and areas of expertise. Once the study contract had been signed in 1992 (see [1] for details of how security was addressed for this contract) the number of interested companies and consortia reduced to about 90 of which 64 made a positive "Expression of Interest". Because of the size and cost of the programme, it had to follow European Community open procurement rules, despite its defence nature. To reduce the selection task, it was considered essential that potential contenders showed that they met certain pre-qualification criteria. These criteria covered: corporate capability and capacity; relevant experience, and management practices. From the security viewpoint we were looking for previous experience with the UK security evaluation and accreditation process, but we would have accepted experience in another process (for example, the US NCSC system) instead. After pre-qualification, twenty three copies of a Request for Information were issued to industry, but only 10 replies were received. By this point, well known names in the European IT industry were beginning to join together to form consortia.

STATEMENT OF REQUIREMENT

The next phase was to issue a Statement of Requirement (SOR). This document provided suppliers with a broad statement of the LITS Prime Systems Integration requirement and invited responses which would demonstrate broad approaches to meet the requirement. The security section described the work being undertaken during the study phase and provided general guidance on requirements. These security requirements were intended to be architecture independent. In particular, although a range of classifications of data and user clearances had to be handled, we did not consider that a multi-level system would necessarily be feasible within the timescale from the programme. Thus, we ensured that a solution based on the use of two or three interconnected system-high networks would also be acceptable. The need for the total system to be evaluated using the European Information Technology Security Evaluation Criteria (ITSEC) was clearly stated. Assurance levels derivations for a reference architecture were provided to enable the suppliers to gauge the likely actual assurance levels that would be required, since the assurance level is a major driver in the cost and difficulty of a secure development. However, we made it clear that the final assurance levels could only be accurately calculated when the supplier's own technical and security architectures were known.

During this SOR phase our main aim was to identify how well the suppliers understood the security needs of the system. To this end, they were asked to explain how they saw security influencing each stage of the Programme and how they planned to manage the total security process.

Seven suppliers responded to the SOR, with replies ranging between one and four lever arch binders full of documentation. Needless to say, the responses varied in depth and understanding. Furthermore, we discovered that suppliers did not always respond in the format that had been requested. Thus, we found it essential to read every page of the responses and actively search for any aspect pertaining to security. Prior to our reading the responses we had identified specific points that we expected to see in the replies: this was taken from the security information that we had supplied in the SOR. The method we used to review the documents was for the LITS Strategic Security Team, comprising a RAF officer and two security consultants, to read each of them independently and highlight any matter with security relevance and also mark where we believed that security should have been mentioned. Our prepared list was then independently compared by each of the reviewers against the high-lighted responses and scores were allocated together with supporting comment. These score and comments were then collated and we held a meeting to discuss the findings. After this meeting, where we were not necessarily in total agreement, the final consensus of the scores fell within the normal distribution curve. Our conclusion was that from the information security point of view, the bulk of the submissions were acceptable but not particularly of a high standard. We concluded that many of the suppliers had not taken full cognisance of the statements we had made in the security section of the SOR.

Because of the importance all levels of management attached to security, it was considered essential that at any time during the selection procedure that if any bidder fell short of a minimum security requirement, then irrespective of other criteria, that bid should fail. However, security was not the only reason why companies failed to be selected to move to the next stage of the competition and this veto was not required. Four consortia were selected to bid against the a more detailed Operational Requirement (OR) which would become the basis for the contracts.

SECURITY EVALUATION STRATEGY

A particular key decision that we had to make before release of the Operational Requirement concerned the security evaluation strategy. Because LITS handles classified data, it must be *accredited* for live operation by the RAF Security Directorate. As LITS will rely at least in part on security measures built into system software and hardware, it is clear that the accreditor will require a certificate of successful system security evaluation under the UK IT Security Evaluation and Certification Scheme.

Within this ITSEC-based scheme, a distinction is made between the *sponsor* of an evaluation (the organisation that commissions and pays for an evaluation) and the *developer* of the relevant system. Within the overall LITS procurement strategy, it was open to us either for the RAF to act as evaluation sponsor, and require the PSI as developer to deliver a system ready for evaluation, or for the RAF to require the PSI to act as both evaluation sponsor and developer, and deliver a system that was already evaluated and certified.

Both of these approaches have benefits and drawbacks. Within the LITS Strategic Security Team, we established that no system with the timescales, size and complexity of LITS had yet been formally evaluated within the UK using either approach. Thus we would inevitably be breaking new ground. In consequence, security evaluation was a major potential risk to the project. We therefore performed a special risk investigation study, specifically addressing the security evaluation strategy.

We determined that if the PSI sponsored the evaluation, it could be difficult for us to monitor its progress. The evaluation facility and Certification Body treat evaluation information as privileged, not discussed with outsiders. In practice, the formal evaluation certificate is always supported by an evaluation report containing observations and qualifications deduced from the evaluation process. The accreditor uses this report in reaching his formal accreditation decision, and may demand additional security measures, either technical or procedural. A delay in obtaining accreditation whilst such measures were put in place would have serious implications for the RAF, and early visibility of evaluation problems was therefore essential.

On the other hand, a major element of the LITS procurement strategy was to pass as much development risk as possible to the PSI. If the RAF sponsored evaluation, we would become a “piggy in the middle” between the PSI and the evaluators. For example, developer effort improving poor quality documentation can often be traded for additional evaluator effort working from the original poor documentation. However, the PSI would have no incentive to take part in such developer versus evaluator trade-offs. Similarly, evaluation was likely to require access to low level proprietary information. The PSI would have little incentive to ensure such information was promptly and efficiently made available to the evaluators.

Within the UK, evaluation is only performed by specialist commercial organisations called Commercial Licensed Evaluation Facilities (CLEFs). Since there are only four companies that own CLEFs, we held discussions with all four to obtain their views on the best way to commission the evaluation. We also discussed evaluation issues with the management of the UK Certification Body, the organisation that runs the UK Evaluation and Certification Scheme.

The major feedback that we received from the CLEFs was that security evaluations usually run into trouble because insufficient consideration is given to the IT security requirements within ORs and subsequent development contracts. The CLEFs felt that this was more important than who sponsored evaluation. It was emphasised to us that developers only placed the same importance on security in their tenders and actual developments as was placed in the customer's OR and contract documents. The choice of evaluation sponsor was less important than ensuring that contracts obliged the developer to provide a system that would be easy to evaluate. For example, any security evaluation requires timely access to the low level documentation of the system, usually including access to proprietary

information that is not generally made available to customers. The developer must be made responsible for providing this information to the CLEF for the initial security evaluation, regardless of who sponsors and controls the evaluation. After completion of the development contract, there will be a need to maintain the system, which could result in a subsequent re-evaluation, in which neither the original developer or CLEF need be involved. Thus the developer's contract must ensure that all necessary information is not only made available for the initial evaluation, but also retained and guaranteed available, in a usable and understandable form, for subsequent re-evaluations, by the same or a different CLEF.

Following completion of our risk investigation study, the decision was made to make evaluation the responsibility of the PSI as part of the development contract. By devolving the responsibilities of evaluation sponsorship, we also devolved control of the evaluation. This meant that the RAF could no longer decide or influence the selection of the CLEF, or set the timing and division of the evaluation work to fit in with RAF constraints and availability. Once work started, it would be inevitably be easier for the PSI to conceal problems, if he chose to do so. However, it was felt that these risks were outweighed by the devolution of the risks and workload of sponsorship to the PSI, who after all would be chosen for his capabilities to accept risk and manage such responsibilities. Moreover, it was felt that evaluation might progress faster if the RAF was removed from the problem reporting and resolving loop as an intermediary between the developer and evaluator. None of the other potential technical and management risks that were identified had clear cut solutions that favoured one approach or the other. Our decision was supported by all the CLEFs, who believed that their relationship with the PSI as developer would be better if the PSI also sponsored the evaluation.

We recognised that there was still a need for evaluation-related work to be undertaken by the RAF to reduce the risk of potential problems in obtaining accreditation. This included an evaluation co-ordination and monitoring task, maintaining strong contact with the Certification Body and the CLEF chosen by the PSI. To ensure visibility of potential evaluation problems, it was decided to make it a contractual requirement for all formal correspondence and reports between the CLEF and PSI to be copied to the LITS Strategic Security Team, and for us to be invited to attend all formal evaluation progress meetings.

We also realised that successful accreditation may depend on demonstrating the presence of physical or procedural security measures which are outside the control of the PSI to provide. The LITS Strategic Security Team retained a responsibility for specifying, organising and managing the provision of these measures by the RAF. This risk to successful accreditation could not be passed onto the PSI, regardless of who became the evaluation sponsor.

The CLEFs also advised us that we would need specialist advice to look at security evaluation aspects of the OR responses. They believed that PSI bidders might put forward technical architectures or implementation plans that would require unnecessarily high evaluation costs, or long evaluation timescales, or perhaps might even be impossible to evaluate successfully. The CLEFs argued that as they were primarily concerned with security evaluation and regularly saw and suffered the consequences of such problems, they were the best source for this advice. However, they also acknowledged that appropriate expertise could be obtained through the regular LITS Management and Technical Support (MTS) contractors, already chosen to support the RAF during the procurement process. After consideration, we felt that raising a separate bid evaluation contract with one of the four CLEFs, solely for security evaluation, would have disadvantages. It would be contrary to the general LITS approach of using the services of standard support contractors, chosen for their demonstrated expertise in relevant areas. More importantly, a conflict of interest could arise should the contracted CLEF also be approached to advise one of the suppliers that had responded to the SOR. With only four CLEFs in the UK, and seven suppliers initially under consideration to receive the OR, the latter point was a potentially serious restriction to free and open PSI competition.

OPERATIONAL REQUIREMENT

Before the OR was drafted it had been decided that the Prime System Integrator (PSI) would be required to bid for two separate but linked contracts: an integration and development contract, and a support contract including facilities management (FM).

The OR was initially drafted by the study contractor by taking the detailed user requirements and turning them into desirable and mandatory requirements. We noticed that this would be limited in scope and would only cover the development of the first tranche of the complete LITS programme and would not include the overall integration and FM aspects. The LITS Strategic Security Team decided to hold a "brain-storming" session to identify from a top down approach, what we would require from the two contracts. Clearly there was some overlap, but we identified many additional requirements to those stated by the study contractor. These additional requirements included maintenance of the security evaluation certificate and security in the project management. This latter point mirrored the requirements imposed on the study contractor (see [1]) to include and identify their own security assurance coordinator and security team leader.

One of the deliverables from the study contract was a System Security Policy (SSP) [2]. This document was drafted without knowledge of the final architecture and thus had many areas that needed to be defined. However, it was a high quality document that received endorsement from the LITS Strategic Security Working Group. This document was included as an annex to the OR and mandated on the suppliers. During the drafting of the OR it was decided to provide the four potential suppliers with draft versions of the document to enable them to plan their approach rather than withholding the document until it was finally ready, leaving only a few weeks for them to prepare their replies. During this drafting period the bidders were encouraged to discuss their ideas and worries with the RAF LITS team.

The major security requirement in the OR was very simple to state: to produce a system that complied with the SSP. In general, no other security requirements or constraints were imposed on the developer by the OR, with some small but important exceptions. The increase in classification of aggregated data over its constituent elements is often a real problem in real systems. This was investigated as part of the security component of the LITS Full Study, and put to the users to canvas their views. The system users came up with a concept that they called "cones of visibility", where each class of user could be assigned to a conceptual cone of data, within which they could perform data analysis and aggregation without cause escalation of classification of the overall results. These cones were in some cases geographically based, in others equipment-type based. However, in all cases the users were able to devised rules that could be applied by an automated system to keep a user's queries within his permitted cone. In relational database terms, these constraints could be likened to schemas and sub-schemas. The PSI was required by the OR to support and implement the "cones" concept.

The OR required the developer to implement the Tranche 1 applications and also provide an infrastructure for the other tranches. In was known that in Tranche 2, there would be requirements to exchange data with external systems holding labelled data, and also for automated grading of printed output according to content. This latter requirement was seen as essential, even if a system-high approach was taken to the architecture. Without security classification labels, all printed output would have to be visibly labelled at the system high level, unless downgraded on the system immediately prior to printing, or manually downgraded after printing by an authorised person. This was seen as a huge management overhead as it was expected that at least fifty per cent of the data would be unclassified. We also saw the imposition of data labelling on the PSI's infrastructure as a way to ensure "future proofing" of the infrastructure to support Tranche 2, when it was subsequently developed. The OR therefore mandated data labels on all data held within the LITS database. However, since all users within a particular area would be cleared for all data related to their applications, a system high mode of operation would still be possible, and we would not be imposing any mandatory access controls (MAC). Suppliers found this difficult to understand and challenging. They were not sure if we intended to impose a CMW-like solution. Indeed, in response one supplier initially proposed CMWs for use as terminals throughout the system. Whilst we were not allowed to specifically coach suppliers, we did point out that their solution could be very expensive and ask them if they were sure that they fully understood the requirement. In reaction to their subsequent query , we were able to expand and clarify this requirement as an addendum to the OR sent to all bidders. In the end, the labelling requirement was satisfied without major difficulty by all the suppliers, either by proposing a C2 functionality DBMS where an explicit extra column was added to each multi-level table for the labels, or by using a B1 functionality DBMS and turning off MAC checks.

An additional requirement that was included in the OR at a late stage, was for End User Facilities (EUF). These will enable users to manipulate, but not replace, information extracted from the corporate LITS database, for reporting, analytic and extrapolative purposes, using standard office

packages. It was made clear that in this environment the system could not automatically determine the classification of the data produced, and hence it would need to be treated as system high with manual action downgrade if necessary.

The OR gave a careful description of the bidder's required response in the area of security and asked for his proposal to explain eight specific aspects of his architecture. These were:

- Relate the security architecture to the overall system design.
- Show how the security architecture and system design meet the security requirements and the SSP.
- Define the security mode(s) of operation.
- Describe the permitted data flows with the security architecture, identifying any security gateways.
- Identify all trusted processes within the system, defining functions and whether they are bespoke, COTS or customized COTS.
- Identify where untrusted applications would reside within the architecture, justifying why they would not need to be trusted.
- Describe how all COTS components would be integrated into the security architecture.
- Describe the compatibility of any package being proposed with the security requirement.

The bidders were also requested to provide an initial calculation of the required ITSEC assurance level or levels for his system architecture, based on the associated risks. Because the system would need to be security evaluated, certified and accredited we also required a statement of their proposed approach to maintaining security in the long-term, because the system would certainly evolve and change during Tranche 1 roll-out to support multiple sites and subsequently during the development of Tranche 2. Moreover, because of the size and expected development time scale, we considered that interim approval to operate from the accreditor would be essential and a building block approach to evaluation would be needed. Additionally, we asked for the proposed approach to electronic interfaces to other systems, an explanation of the security skills of the consortium, and the identity and qualifications of the staff proposed for key development posts. We also required them to explain their planned approach to evaluation and certification, including their choice of a CLEF, and finally a description of their proposed security administration to include their FM proposals.

During the drafting stage we received very few queries from the tenderers, but we did hold regular meetings with all four consortia usually at their request. Bids were received from all four consortia, and when single copies of each were stacked on top of one another they totalled over 4 feet in height. These were reviewed in the same way as the SOR, by reading every chapter. The format of the responses was rigidly fixed by the OR, which made it much easier for us to identify the security aspects than in the SOR. The replies were required to be set out in chapters on the following subjects: system design, relevant experience, quality, management and planning principles, technical architecture, applications development - methods and tools, applications development - delivery of functionality, implementation and rollout, integration, facilities management, training, documentation support, management of change, security, risk management, delivery capability, compliance matrix. The decision to read each chapter was fully justified as again we found major security conflicts been chapters, which necessitated a total of 50 clarifying technical questions on security being formally asked. An example of the type of conflict we experienced was the plan in the security chapter of one proposal to offer a one-way regulator as the one type of interface between systems, but in the applications chapter the application users were offered on-line interrogation of remote databases on other systems. Another example was the bidder who extolled the benefits of a particular proposed security guard processor in his security chapter, but included a different guard from another company in his costings.

Another frustration was the bidder who provided a description of his security architecture that addressed all of our required points, but in a radically mixed-up and re-arranged order! This was legitimate according to the terms of the OR but took us a lot of time to cross-correlate. Finally, despite clear and precise instructions on what all proposals had to cover, all bidders failed to address at least one specific point in the way that we requested.

Having undertaken the task of reviewing all the chapters we also invited the LITS Accreditor and CESG to review the technical architecture and security chapters. Overall, there was little conflict

between assessors and a clear order was evident. However, from the security viewpoint all bidders were very close in the scoring. All four had proposed similar technical architectures of a two-tiered system-high; one at Secret and the other at Restricted. We did notice that all bids appeared to have severe limitations on the subjects of Electronic Data Interchange, FM and secure gateways. Finally, we recognised that all suppliers would have problems with their solutions but none of the security problems provided a differentiator, and we believed that all the security problems could be overcome. Two of the four consortia were selected to move to the next stage as short-listed bidders.

SYSTEM PROCUREMENT STUDIES

One of the LITS programme objectives is to manage and reduce the risks and uncertainties normally associated with a large IT development. As part of this approach, the two final short-listed bidders for the PSI contract were paid to undertake a number of System Procurement Studies (SPS). These studies were to investigate specific aspects of the bidders' proposals that were perceived by the RAF to represent potential high-risk areas in their proposed system design or development processes. Information security featured as a major driver in two of these studies. As part of the technical architecture study, the security architectures of both bidders were developed in line with expansion of their proposed overall technical design solutions. In a specific information security study, both short-listed bidders were paid to prepare System Electronic Information Security Policies (SEISPs) for their proposed technical solutions, based on the security policy documentation produced by the original Full Study contractor. In accordance with normal UK MOD procedures for secure system development, SEISPs are used to define the technical security measures to be incorporated within the trusted hardware and software of a system. However, normally, the SEISP would only be produced following an actual implementation contract award.

Both of the above studies achieved their objective of reducing potential contract risk. We also found them useful as a tool to assess the general strengths and weaknesses of the two competing security teams, in a way that is not normally possible, as we were able to see the two teams at work solving real problems. This provided a valuable insight into the maturity and technical knowledge of the individuals who might subsequently be leading the information security aspects of the LITS programme. However, although we had become conversant with the skills and knowledge of these specific individuals, neither consortium was able to guarantee these teams would continue unchanged with the work once a contract was let.

The two short-listed consortia had similar, but not identical, proposed security architectures. In both cases the LITS system would comprise two distributed system high networks, running at System High Restricted and System High Secret respectively. In addition, there would be electronic links to other RAF and UK MOD systems. The two system high networks would be linked electronically through distinct secure Guard systems ("firewalls"): external links would vary from tape transfer to on-line electronic links protected by secure gateways. One bidder proposed to combine the functions of the inter-network Guard and the external electronic gateways through provision of a single generic Guard system. This offered the potential for major savings in architectural complexity and in hardware costs. However, the relevant system procurement study demonstrated that this architectural solution not only added major complexity to the Guard system internal design, it also increased the ITSEC evaluation level required for the Guard. The associated additional development and evaluation costs caused the bidder to switch to a solution based on separate hardware for the two distinct functions.

One unexpected finding from the SPS work was that a number of the other study areas, which appeared to have little direct IT security relevance, produced results which had major implications for the security architecture. Often the relevant security team were unaware of these implications. For example, data migration from the existing unclassified mainframe-based supply system proved to be conceptually complex due to the need for reverse data transfer from LITS back to the mainframe system during the period when some locations had migrated to the use of LITS whilst other locations were still connected only to the existing supply system. One contractor could only support this through a major last-minute modification to his proposed security architecture. There were clear benefits to the RAF in exposing such programme risks at this early stage.

CONTRACT NEGOTIATIONS

Contract negotiations were started with both consortia before the end of the SPS phase, for both a PSI contract and a Support (FM) contract. Many contract schedules had to be written as well as the general Terms and Conditions. The LITS project office decided early on in the work that certain of the schedules would be drafted by the RAF and others by each of the consortia. The decision was made that the two security schedules should be drafted by the consortia. However, in order to ensure some degree of completeness, we compiled a list of all those aspects that we considered should be covered by each of the contracts. We thought that having the bidders doing the work for us was the easy option. However, we soon found the opposite was actually the case as we were having to keep track of four entirely different contracts, because each consortium had different views of what was needed. Furthermore, the approaches taken by the two consortia were radically different: one consortium's negotiator was a Infosec man, the other had little security knowledge but was experienced in contract negotiations. This was evident from the former appreciating that security documents, such as SSPs, are living documents which need to expand and develop as technical solutions are decided, whilst the latter favoured fixed baseline documents, after which formal contract amendments would be required if the documents were changed. The difficulties with this approach were exacerbated by the necessity to negotiate the contracts before the end of the SPS work. Thus, we were being asked to agree that the contractually binding baseline security documents should be those that were developed during the SPS work, at a time when these had not completed or fully reviewed.

We also found that British Government contract “standard” terms and conditions, which have been used for many decades, did not match the LITS procurement strategy and again the standard security conditions had to be studied to ensure that we were agreeing to the correct requirements.

We were also concerned that other schedules would impact on the security aspects of the contract. We therefore asked to be allowed to review all the schedules as there were being drafted. With 46 schedules for each of the PSI contracts and 23 schedules for each of the Support contracts, and taking into account that not only were these schedules changing daily because of the negotiation, but also the standards for schedule layout, wording and contents were still being developed, we soon realised that this task was much greater than anticipated. The solution we proposed was that in the overarching Terms and Conditions part of the contract we would insert a statement to the effect that if there was any conflict between the security schedule and any other schedule, then the security schedule would take precedence. This proposal was accepted by the central contract drafting team and certainly saved us a lot of work and worry. Now that we are working within the terms of the PSI contract we have found that this action has been worthwhile.

TRANCHE ZERO PROJECTS

Because of the long timescales for the LITS Programme, it was decided that implementation of two LITS applications should be initiated before the main LITS Programme, as self contained projects. In both cases, there were urgent short-term requirements that could not be met satisfactorily by existing IT systems. The early implementation of these two systems as a conceptual LITS Tranche Zero would provide tangible benefits that would outweigh the potential economies obtained by delaying implementation until they could be included as part of the full LITS system. One project was to develop a Warehouse and Transport Management System (WTMS) for the RAF equipment storage depots. The other was to provide a fully automated system for the introduction of new weapon systems into service. This latter project, entitled Logistic Support System {LSS) was initially planned to aid the introduction of the Eurofighter 2000 (previously known as EFA) into the RAF. For both of these projects independent and autonomous project offices were set up, although still under the control of the LITS Programme Board. However, the LITS Programme Security Team has been fully involved with both projects from their inception.

For WTMS, we were instrumental in providing advice to the project office for the security chapters of their OR. Subsequently, we have provided a WTMS Security Assurance Coordinator (SAC), a role defined under the PRINCE project management philosophy used by the RAF to monitor security aspects of a contractor's performance (for further details see [1]), and also an independent security consultant to the WTMS project office. We are also responsible for monitoring the security evaluation of the system currently in progress by one of the UK CLEFs and we attend a formal security working group set up to monitor the security development. This system is being developed as a self-contained

system handling only unclassified data. However, we know from our Full Study that in the future it will need to be integrated into the LITS system and current thinking is to expand it throughout the RAF to handle consignment tracking. Therefore, we have insisted that security to the assurance level of the LITS Restricted network should be incorporated from the start, and we have ensured that all security development has been compatible with our main Programme.

LSS, on the other hand, to satisfy its own operational requirements must process classified data up to and including Secret, and must also directly interface with industrial supplier systems for the purposes of Electronic Document Interchange (EDI), primarily to provide electronic ordering and invoicing functions. Under current UK guidance, it would be impractical to build a single homogeneous system containing both these facilities. Thus, the architecture chosen for LSS has two tiers: one running MLS to Secret and the other at unclassified, with the two tiers linked by a guard processor. The EDI functions and links are located on the unclassified tier. In addition, because of concerns over indirect access to the Secret tier from external systems via the unclassified tier, a trusted message filter will monitor all incoming external traffic to ensure that only recognised, properly formatted, EDI messages are accepted. The inter-tier guard processor will also mediate on the distribution of data from the Secret tier to users who do not have a need to see all classifications of data held on that tier. For example, users on certain sites will only be allowed to access data up to Confidential. However, because it is known that there will be some incompatibility between the classifications and labelling of data on the full LITS system and LSS, it has been necessary to make a conscious decision to leave the development of a way to integrate LSS into Tranche 2 of LITS to the future. This risk has been accepted as a necessary consequence of not delaying the LSS development until the LITS labelling schema was finalised. The LITS Strategic Security Team has been involved with LSS from the start of the LSS study and has provided the LSS SAC, assisted with the evaluation of LSS bids, and latterly provided independent security advice to the project.

LESSONS LEARNED FROM TRANCHE ZERO PROJECTS

The involvement of the LITS Strategic Security Team in these early start projects has meant that the lessons learned solving their practical problems can be incorporated into the main LITS Programme. For example, we are only just starting our first real involvement with the LITS CLEF. However, we have been dealing with two different CLEFs for WTMS and LSS for several months, and are now quite comfortable with CLEF requirements and difficulties.

We learned an important lesson early on during the LSS project, namely that the SAC should not just read and comment on security deliverables. It is essential that the SAC reads all contractor documents to ensure that security is fully covered and, just as importantly, to confirm that where it is claimed that there are no security implications, this is a valid statement. We also observed that it is a mistake to contract specialist security consultants just to produce security documentation. We discovered that this led to decisions being taken elsewhere within that study team without any security assessment or involvement, and by the time these documents reached the SAC, it was too late to easily change poor design decisions where security implications had been missed.

Finally, these early start projects taught us some useful practical lessons about the real world of commercially available security products. Just because a product is on an Evaluated Products List, it does not mean that it is readily available on the market to be purchased, or that it can be easily integrated into a state of the art system. Secure versions of all the major DBMS packages are now available. However, database designers do not necessarily understand the full implications of the security features in these packages or the impact of these features on end users. The major secure DBMS products solve security problems in different ways. Even knowledgable security experts may not have a detailed appreciation of the crucial differences that exist in the legality and semantics of the security functions within these products, and be able to make an accurate assessment of the best approach for a particular product and system.

GENERAL LESSONS LEARNED

LITS will be a very large system handling large quantities of both classified and unclassified data. Because of its size and integrated nature, IT security was seen from the start by senior management as being a major potential project risk. With hindsight, this was a correct decision.

At an early stage, we realised we would have to modify the normal UK MOD IT security standards and procedures to meet our particular procurement requirements. This was the correct approach.

Under the LITS procurement strategy, the Full Study and PSI contractors are responsible for requirements analysis, system design and system implementation. The LITS security team followed this philosophy. We tried not to interfere, we only asked questions or provided them with answers to policy questions. This was also the correct approach. It put the risks and responsibilities firmly with the contractors. System security evaluation is a particular problem area under the UK approach, where defence evaluations have to be contracted on a commercial basis. The objective has to be to ensure that the system achieves accreditation for live operation, not merely that it passes evaluation.

Our security risk reduction studies worked well. Normally, a bidder is not able to address the problems you find in his proposal until after he has been awarded the subsequent contract. With the LITS approach, the two short-listed bidders had a very strong incentive to put things right, as we still had a choice of going elsewhere.

It is important that overall control of security remains with the customer. There are many security consultants available but each individual has their own expertise and weaknesses. When choosing a consultant it is important that the right one for the task in hand is selected, and during a procurement phase it is essential to obtain advice from one who understands the technical issues and the security implications.

We were told by one contractor that bidding for Government work is like trying to pass an examination. He then commented that the LITS security team was trying to make the examination even harder!

CONCLUSIONS

The main conclusions that we came to after this phase of the LITS Programme was completed was that security permeates through all aspects of a secure IT system and is especially important during the procurement stages. A coordinated and consistent security approach throughout a project is important. It is also essential that nothing is taken for granted and everything is checked, as we have tried to do. A final backup is to have an overarching policy statement that provides for future conflict being settled on the side of security, if security is that important.

ACKNOWLEDGMENTS

The authors would like to express their thanks to the other members of the LITS Strategic Security Team, A G Klein and G Martin, for their assistance in the production of this paper.

REFERENCES

[1] R J Kennett and M J Nash, “Information Security in a Complex Defence System Procurement: A Personal Management Experience”, Proceedings 5th Annual Canadian Computer Security Symposium, Ottawa, Canada, 1993.

[2] M J Nash and R J Kennett, “Security Policy in a Complex Logistics Procurement”, Proceedings Ninth Annual Computer Security Applications Conference, Orlando, Florida, USA, 1993.