



## **MANAGEMENT AUDIT UNIT**

### **CUMBRIA POLICE INTERNAL AUDIT REPORT**

#### **NETWORK SECURITY & CONTROLS FOLLOW UP**

**Draft report Issued:**  
**Report Issued:**

**July 2005**  
**August 2005**

## 1.0 INTRODUCTION

- 1.1 The purpose of this follow up was to review progress on action taken by the Constabulary to address the recommendations from the audit review of network security & controls carried out in 2004.
- 1.2 The following members of staff provided information during this follow up:
- Nathan Parry, Director IT/IM
  - Craig Goodfellow, IT Network Team Leader
  - Ann Bell, Information Security Officer

## 2.0 OVERALL EVALUATION & CONCLUSION

- 2.1 **Eight recommendations were made as a result of the previous audit review; 5 of which were grade 1 recommendations. Generally, those items agreed in the action plan to be completed by April 2005 have not yet been completed: progress is ongoing and the internally set target dates for completion have now been revised to October 2005. Of the grade 1 recommendations:**

- All are in the process of being actioned [1 is dependant upon the wider Cumbria Constabulary business continuity project that has recently commenced]

**Of the remaining 3 recommendations [all grade 2]**

- 1 is in the process of being actioned but is dependant upon progress with the new HR system
- 2 are in the process of being actioned as part of the general CJX accreditation [target October 2005].

## 3.0 FOLLOW UP TO THE PREVIOUS AUDIT REVIEW

- 3.1 The recommendations made during the last review have been followed up, as below:

RECOMMENDATION & GRADE	ACTION TAKEN / COMMENTS	
<p>R1 The network security policy [including determination of risks and steps established to deal with these] should be progressed as a matter of some priority: it should include how potential threats from (e.g.) viruses, hacking etc. are controlled. A set of procedures should be established to identify the level of security monitoring that should take place. [Grade 2]</p>	<p>In Progress</p>	<p>The completed action plan of the original 2004 MAU report had a target for completion of these aspects by April 2005.</p> <p>Whilst separate working procedures/rules in respect of some control elements exist and are available on the network for general viewing, we understand that the overall policy is to sit within the wider framework of CJX accreditation &amp; policy. This is targeted for completion by October 2005. Discussion with the Information Security Officer noted that a <i>draft</i> is expected by October. However the Information Security Officer will need to be advised by, and have procedural drafts on some aspects from the IT unit in order to incorporate these into the overall framework.</p> <p>The separate internet policy has been reviewed in the light of a review</p>

		<p>commissioned by the Constabulary &amp; carried out by Network Defence (supplier). This reviewed the configuration as recommended by the suppliers. A report was produced and considered by COG.</p> <p>There had been views expressed within the constabulary that the existing scheme was too restrictive, however after careful consideration a decision has been taken not to change the existing policy.</p>
<p>R2 A policy should be established setting out the firewall rules that should be in place. This should ensure that the machine policies reflect the management requirements of the Constabulary and reflect a “top down” approach. [Grade 1]</p>	<p>In progress</p>	<p>As for R1: target October 2005. There has been some progress, initiated from within the network section. This has been specific to Remote access tokens.</p> <p>These tokens, together with individual logon ID’s and passwords provide the necessary level of security access from laptops. The Network support Officer has carried out an internal review of these: their current validity and necessity. There are in the region of 100 of these tokens available to IT staff and suppliers. As a result of this, the network section has produced a draft internal procedure. This envisages a regular 6 monthly review of this aspect. Further work is necessitated and this is to be incorporated into the overall formal re accreditation policy to be produced by the Information Security Officer [see above].</p> <p>The wider issue of firewall rules, ports open to whom, who can create/amend/delete firewall rules has still not been drafted.</p> <p>Internal change control procedures have been established: these relate to any changes that potentially affects service delivery or functionality. They are intended to provide a formal record of requests, authorisation and action, including notification to appropriate staff of the changes to take place and how it affects them. [E.g. system down time].</p> <p>We understand that Network Defence have been commissioned to carry out an overall risk assessment of the firewall rules and port accesses. This is linked to the implementation of the case &amp; custody application that is</p>

		<p>currently still in test stage but expected to go live once the review has been completed.</p> <p>This is an important issue that requires closure with a set of procedures regarding firewall rules. In particular: the procedures regarding who can add, amend and delete firewall rules.</p>
<p>R3 Establish a more efficient formal method of notification (leavers) from managers to IT section to terminate network access. (Grade 2)</p>	<p>Ongoing</p>	<p>Whilst this recommendation was not considered by Internal Audit to be of the same significance as firewall rules it was reported as an ongoing weakness. It was explained to us during the original review that a satisfactory solution would be provided by the establishment of a more robust HR system. This would automatically link to the active directory and disengage leavers from their network access rights.</p> <p>Whilst the core HR system has been implemented across the Force, there are still issues that need to be resolved.</p> <p>We are given to understand that IT will own both the system and the administration of the system and that a link to the active directory has now been proven. However, the business owner is Human Resources and this particular issue is not considered by IT as an IT issue: rather an HR issue. In effect the links are enabled, but will not be operated until the necessary data elements within the HR system are fully operational and data quality can be assured.</p> <p>It was explained to audit that the old system is to be switched off in October 2005 and we understand that there exists a specific project on data quality. Once this is completed and data assurance provided, the feed to active directory should be activated.</p>

RECOMMENDATION & GRADE		ACTION TAKEN / COMMENTS
R4	Supplier/contractor activity from within Force buildings should be supervised. A risk index of suppliers and which network activities they relate to should be established and connectivity should be monitored according to the risk index. (Grade 1)	<p>In Progress</p> <p>The action plan regarding this recommendation notified that a new vetting officer was to be appointed and a new identity badge system had been purchased and was currently being implemented. This, together with a review of establishing a supplier index is to be completed by October 2005.</p> <p>It has been explained to MAU that ad hoc contractors currently use the same badges as visitors. Longer-term contractors use the same badges as staff. These badges are issued after security clearance checks have been carried out. There has therefore been no change to this aspect at this point in time.</p> <p>We understand that the Vetting Officer post has not yet been filled.</p>
R5	A check of current firewall rules should be undertaken as priority and the appropriateness of rules against policy (R2) considered. (Grade 1)	In progress See comments above [R2]
R6	Formal change control procedures for firewall rules should be established and access to set, amend or delete these rules tightly controlled. (Grade 1)	In progress See comments above [R2]
R7	Formal rules for individual supplier remote access should be established and supplier agreement recorded. (Grade 2)	<p>In progress</p> <p>The original agreed completion was in accordance with CJX re accreditation timetable of April 2005. This is now October 2005.</p> <p>We understand that this is also linked to the appointment of the Vetting Officer.</p>

<p>R8 A formal contingency and business continuity plan should be established. This should be based on identified risks and prioritised accordingly. It should include a worst-case scenario of the whole HQ building becoming inoperative, actions to be taken, key contacts and knowledge &amp; actions required. (Grade 1)</p>	<p>In progress</p>	<p>At the time of the original audit report The Director of Corporate Development [now Director of Strategic Development] had been tasked by business Management Board with business continuity.</p> <p>We understand that this project has now just recently been initiated and that the IT continuity plans should sit within the overall Constabulary's plan.</p> <p>IT has recently demonstrated that recovery from a disaster [Carlisle floods] was successful in bringing back facilities and systems efficiently. The argument has again been put forward by the force that these actions, and the fact that staff know what to do in effect reduce the need for a formal plan.</p> <p>However: whilst accepting this success, it must again be noted that this is reactionary recovery due in part to knowledge and well experienced IT staff. There exists specific re build instructions for hard and software.</p> <p>What does not exist is the forward plan: the more generic view of what should happen within scenarios that have been considered and risk assessed. For example in the worst-case scenario: the whole Carleton Hall complex becoming immediately inaccessible/destroyed.</p> <p>A formal plan should consider varying degrees of risk, their standing in order of importance [impact and likelihood] and cascading detail according to each scenario.</p>
---	--------------------	---