COMPUTER SECURITY REVIEW

SOUTHERN REGION

19 March 1993

Report issued by:

Miles Jordan
Audit Manager
(Projects & Computing)
19 March 1993

REPORT TITLE: Computer Security Review

REPORT NO: SN / 004

AUDIT OBJECTIVE: To assess the security of computer systems in the Southern Region including measures taken to protect NRA data and software and an assessment of site security.

TO: Kevin Whiteman
Regional General Manager
Southern Region

FROM: Miles Jordan

DATE OF AUDIT: May 1992

REPORT DATE: 19 March 1993

AUDITOR: Kevin Woodrow — Principal Auditor

AUDIT MANAGER: Miles Jordan — Audit Manager (Projects & Computing)

CIRCULATION:
Nigel Reader, Director of Finance
Kevin Bond, Director of Operations
John Ashworth, Head of Systems Development
Ken Hodgson, Finance Manager
Peter Stafford, IS Manager
Steve Egan, Head of Internal Audit
Marion Adkins, Audit Manager (South)

CONTENTS

1.0 INTRODUCTION

1.1 Computer systems are integral to the operation of the Authority, both Nationally and within each of the Regions.

1.2 The 1992/93 Operational Internal Audit Plan contains a review of measures taken to protect NRA data and software, including an assessment of site security. Therefore, it entails a review of all the Regions and of Head Office. The Audit Plan has been approved by the NRA Board.

1.3 The Southern Region has a number of different computer systems running various applications important to day to day operations.

1.4 In addition, the Region has contracted with IT Southern Ltd, a member of the Southern Water group of companies, for the Company to supply computer bureau facilities operating important applications.

1.5 This audit report details the findings of the audit work performed on computer security in the Southern Region.

2.0 SCOPE AND OBJECTIVES

2.1 Scope

The audit reviewed existing computer security arrangements in the Region with the aim of reporting on the following areas.

- Strategic planning
- Physical security
- Development and maintenance
- Operation and backup procedures
- Data security
- Continuity of operations (excl. contingency planning)
- Networks and remote access
- Logical access control
- Staffing issues
- Legality of software copies
- Sensitive applications

In each case the work covered the in-house computing facilities at the Region and to the extent to which Internal Audit was able to gain access, the bureau facility which the Region uses at IT Southern Ltd.

2.2 Objectives

The objectives of the audit were to highlight weaknesses and to recommend practices which will enable management to increase the efficiency and effectiveness of computer security within the organisation.

3.0 CONCLUSIONS AND SUMMARY

3.1 During our review of the computer systems of the Southern Region we found the general level of security to be good given the nature of the operation of the Authority and of the computer systems operated by the Region.

3.2 We did, however, identify some areas where there are weaknesses in controls, the strengthening of which would benefit the Region.

3.3 There are three weaknesses which we consider should be addressed immediately.

3.4 The first of these relates to the removal of the access of staff who leave the Authority to the NRA computer systems running at IT Southern Ltd. At the time of this review four users of the system were found to have left the NRA between 10 days and 7 months previously. We recommend that the system of notification of leavers from Personnel to IS and on to IT Southern be revised so that users are removed from all systems at the end of the day when they leave the NRA. We also recommend that monthly comparisons of the mainframe user list and establishment list are conducted so that management can gain assurance that no non-NRA staff have access to the system.

3.5 Secondly, no backups of the VAX systems are stored off-site. We recommend that a form of off-site storage be implemented.

3.6 Thirdly, the Computer Room at Guildbourne House contains no fire fighting equipment. We recommend that a hand held fire extinguisher be placed in the Computer Room immediately.

Physical Security

3.7 The Computer Room at Guildbourne House has two doors secured by mortice key locks. We recommend that replacement of the locks with a swipe card system and an automatic closing mechanism be considered.

3.8 A number of non-operations staff have access to the Computer Room. We recommend that access be restricted to operations staff only.

3.9 Computer equipment located in at least one site is housed with communications and printing equipment. This results in access of non-operations staff to computer equipment. We recommend that computer equipment be housed separately and access be restricted to operations staff only.

3.10 Access to Guildbourne House depends on knowledge of the access number to a keypad lock on the reception door. It is considered that key locks are not as secure as swipe card systems and that such systems have additional advantages. We recommend that replacement of the keypad lock with a swipe card system be considered.

3.11 The Computer Room at Guildbourne House contains a single smoke detector and no fire fighting equipment. We recommend that a thorough review of the fire detection and fire fighting requirements of the computer areas at each site of the Region be undertaken.

3.12 We noted the siting of the Guildbourne House Computer Room on the floor below the staff canteen and kitchen. We recommend that, should the siting of the Computer Room be reviewed at a future time, consideration of the risk of flood should be made in selecting a new site.

3.13 The Computer Room is air conditioned to maintain the temperature within working limits of the equipment. There is no alarm if these limits are exceeded and the conditioning system has failed twice within the last four months. We recommend that a temperature sensor be installed and alarmed to the Control Room to sound if preset limits are exceeded.

3.14 The Computer Room does not have an Emergency Power Off button which is essential to cut power to all systems should a fire develop. We recommend that such a button be installed.

Development, Acquisition and Maintenance

3.15 A development staff member has access to the live environment. We recommend that access to the live environment be restricted to operations staff which may include a Database Administrator with no development responsibilities.

Operation and Backup Procedures

3.16 Although there are a number of documented procedures there is no complete operations procedures manual for the systems of the Region. We recommend that such a manual be drawn up.

Continuity of Operations (excl. Disaster Planning)

3.17 A number of items of equipment, including computers, in the Region are powered through an Uninterruptable Power Supply (UPS). The UPSs are currently not subject to a formal maintenance agreement. We recommend that such a formal agreement with a specialist third party be entered into.

Networks and Remote Access

3.18 The Region has a number of dial-in modems to the VAX systems which are not secured by a dial-back device. We recommend that such a device be implemented.

Logical Access Control

3.19 Users of PC networks are currently unable to change their passwords without aid from IS, are never forced to change their passwords and are not required to use a minimum length of password. We recommend that the configuration of the network software be changed so as to incorporate these facilities.

3.20 Access to the Regional Emergency Control System (RECS) on a VAX computer is gained through modems from area offices. Several control weaknesses are apparent. These relate to information on access to the main systems (eg username and password) which are held on Area Office PCs and may be typed to the PC screen. We recommend that existing measures to request the supplier of the software to remove these security weaknesses be pursued. We also recommend that following amendment individual usernames and passwords are used and that these are not the same as each other.

3.21 A number of users on live environments of the VAX systems have passwords which have long lifetimes. We recommend that users with system privileges have passwords with a life of 30 days and users without system privileges a life of 90 days.

3.22 A number of user accounts on the live VAX systems have not been accessed for a significant period. We recommend that user accounts which have not been accessed for a significant period be "disusered". A significant period may be one month for users with system privileges and three months for users without system privileges.

Staffing Issues

3.23 The Region has appointed a Quality Assurance (QA) Controller who currently reports to the IS Manager. The remit of this post is both to prepare QA policies and procedures and to audit against them. Such audit work requires the auditor to be independent of staff directly responsible for the areas audited. We recommend that this post report outside any function for which it has audit responsibility.

4.0 AUDIT FINDINGS AND RECOMMENDATIONS

4.1 Strategic Planning

Strategic planning at the Regional level appeared good.

A Regional Information Systems Steering Group (RISSG) has been established which meets regularly to determine local policies and procedures. Members of the RISSG are also members of the National ISSG and the Core Business and Support Groups.

Since the audit we understand that the RISSG has agreed a Regional IS Controlling Framework.

4.2 Physical Security

4.2.1 Computer Room Security

The Computer Room may be entered through either of two doors. The first door gives access from the corridor, and the second gives access from the Control Room which is manned continuously.

Both doors are secured by a mortice key lock. On one occasion when the room was visited during the review the door from the corridor was found to be unlocked.

Recommendation

We recommend that consideration be given to replacing the locks on the doors to the Computer Room by a swipe card lock system and that the doors be fitted with a self closing mechanism.

4.2.2 Access of Development Staff to the Computer Room

Members of staff with access to the key to the Computer Room include development staff, and other non-operations staff.

Recommendation

We recommend that access to the Computer Room be restricted to only those members of operations staff who require access to perform their duties.

4.2.3 Security of Computer Equipment at Remote Sites

We understand that the Computer Room at the Waterlooville Area Office contains four printers and some communications equipment in addition to the computer processors. This results in a number of staff, who are not computer operations staff, having access to computer equipment.

Recommendation

We recommend that access to computer equipment be restricted to computer operations staff. To this end we recommend that the equipment be housed separately from printers to which users have access and, if possible, from communications equipment.

4.2.4 Building Access Control at Worthing

Access to Guildbourne House, Worthing is gained at all times through reception. During office hours the reception is manned and staff are recognised or required to show their NRA identity cards to be admitted. Out of office hours access may be gained by using a buzzer to alert the continuously manned Control Room. Control Room staff identify the member of staff using a video camera and answerphone, and may admit the member of staff to the reception area, using a remote lock release.

From the reception area access is gained to the rest of the building by double doors secured by a keypad lock. The number of the keypad is changed at approximately three to four month intervals or, if following a member of staff is sacked and must be escorted from the building.

Keypad locks have a number of deficiencies. The same access number may be given to a number of people so that access gained may not be attributed to an individual. The access number may also become known to staff who have not been authorized to have it. Some keypads also have design flaws in that they may be opened by different combinations of keys than those programmed to give access.

Swipe card systems enable the access of staff to be traced to individuals. They ensure that those staff with access are those authorized. They do not suffer from the design problems of some of the keylock systems. Finally, a number of swipe card systems exist which may be efficiently controlled from a central PC. They enable access of individual members of staff to be set at certain hours and for certain days. Management, therefore, control access and may ensure that it is restricted to that actually required by staff to perform their duties. The access of a card may also be withdrawn should a member of staff leave not returning their card. Access to a non-member of staff does not then continue, or staff are not required to remember a changed number.

Other regions also combine the swipe card system with an identity card or time recording system.

Recommendation

We recommend that consideration be given to replacing the keypad lock system for access to Guildbourne House with a swipe card lock system. This would have the additional benefit of enabling sensitive areas within the building, such as the computer areas, to be easily further secured.

4.2.5 Fire Detection and Fire Fighting

The Guildbourne House Computer Room contains a single smoke detector situated in the ceiling. This smoke detector is connected to the main fire alarm system.

The Computer Room contains no fire fighting equipment.

Recommendation

We recommend that a hand held fire extinguisher be placed in the Computer Room immediately.

We further recommend that a thorough review of the fire detection and fire fighting requirements of the computer areas at each site be undertaken. This should involve equipment for the detection and automatic fighting of fires within the rooms and within the floor and ceiling voids. Consideration should be given to the fire resistant properties of the rooms themselves.

4.2.6 Risk of Flooding

The Computer Room in Guildbourne House is situated one floor below the staff restaurant and kitchen. The kitchen must be regarded as having a higher risk of water leakage, and hence flooding, than an equivalent area of general office space.

Recommendation

We recommend that, should the siting of the Computer Room be reviewed at a future time, consideration of the risk of flood should be made in selecting a new site.

4.2.7 Computer Room Environmental Control Alarm

The Computer Room at Guildbourne House is air conditioned so that the temperature in the room is maintained within the working limits of the computer and communications systems.

The air conditioning system has failed twice within the last four months with consequently high temperatures in the Computer Room.

There is no alarm system to notify staff when environmental conditions exceed tolerance limits.

Recommendation

We recommend that a temperature sensor be installed in the Computer Room together with an alarm which will sound when the temperature exceeds preset tolerance limits. The alarm should sound in the continuously manned Control Room.

4.2.8 Emergency Power Off

The Computer Room at Guildbourne House does not have an emergency power off (EPO) button.

Such buttons are essential to cut power to all equipment in the Computer Room should a fire develop.

Recommendation

We recommend that an EPO be installed in the Computer Room close to the door. The EPO should be easily reached from the doorway but not positioned so that it may be activated accidentally.

4.3 Development, Acquisition and Maintenance

4.3.1 Access of Development Staff to the Live Environment

A member of the development staff has access to the live environment. We understand that this member of staff fulfils the role of the Database Administrator for the Region.

Recommendation

We recommend that development staff have no access to the live environment. Rather, transfers of code to a live area should be performed by operations, or a Database Administrator with no development responsibilities, following authorization.

We understand that a new post of Database Administrator has been approved. This post will report to the Operations Controller. The recommendation would be satisfied by limiting the access to the live environment to the Operations Controller and his staff.

4.4 Operation and Backup Procedures

4.4.1 Off-site Storage of Backups

Backups of files from the VAX systems are taken and stored in the firesafe in the Control Room. No backups are stored off-site.

Recommendation

We recommend that a form of off-site storage be implemented. This store should contain at least one recent backup of all files of the system at all times.

4.4.2 Operations Procedures Manual

The Region has a number of documented procedures and system reference sheets but has no fully documented operations procedures manual. Such a manual would be an aid in the day to day running of the systems at the Region, acting as an aide memoire to staff familiar with the task concerned, and also acting as an aid to staff unfamiliar with a necessary task when the usual member of staff is unavailable.

Recommendation

We recommend that an operations procedures manual be drawn up to cover all of the systems running at the Region. In doing this we recognise that significant informal material which is already present will be incorporated in the manual.

4.5 Data Security

No findings additional to those cited elsewhere in this report were made.

4.6 Continuity of Operations (excl. Disaster Planning)

4.6.1 Maintenance of Backup Power Supply

The Computer Systems at Guildbourne House are powered through an Uninterruptable Power Supply (UPS). The UPS can provide backup power for several minutes in the event of a mains failure. A second UPS is used in Finance and a further three UPS systems will be purchased soon to support the Sun Workstations in the Water Resources section.

No UPS is currently covered by a formal maintenance agreement. Maintenance has been performed informally by the supplier of the UPS systems.

Recommendation

We recommend that a formal agreement be entered into with a third party to maintain the UPS equipment. For ease of administration this could be drawn up following the installation of the new UPS equipment, provided that this does not result in undue delay in providing formal maintenance cover for the existing equipment.

4.7 Networks and Remote Access

4.7.1 Modem Access

Guildbourne House has a number of modem devices. Of these six allow incoming access for the use of the area offices to access RECS, one allows incoming access for the use of supplier support, the Operations Controller and the future Database Administrator, the third is for the use of other staff.

There is no dial-back security on the access of these modems.

Recommendation

We recommend that incoming modems are secured by the use of a dial-back device.

4.8 Logical Access Control

4.8.1 Withdrawal of Access to IT Southern Ltd Mainframe

A large number of NRA staff have access to NRA systems which are run on the IT Southern mainframe. This system is operated as a bureau facility.

A system exists for Personnel to notify Information Systems when a member of staff leaves the Authority.

We understand that in the past IT Southern removed users from the mainframe system when their accounts had not been used for more than six months. This practice was discontinued at the request of the Authority.

The current list of users on the mainframe system was compared with the establishment list as at 6 May, 1992. Four users were found to have left the NRA between 10 days and 7 months before this date.

Recommendation

We recommend that the system for notification of leavers from personnel to IS and hence to IT Southern be revised so that users are removed from systems at the end of the day when they leave the NRA.

We further recommend that monthly comparisons of the mainframe user list and establishment list be conducted so that management can gain assurance that no non-NRA staff have access to the system.

4.8.2 Password Control on the PC Network

Users on the network may only set their initial password under the supervision of the PC Controller or his assistant.

Users may subsequently change their passwords only with further assistance. They are never forced to change their passwords and are not compelled to use a minimum length of password.

We understand that the network software, Novell, may be configured so that users are forced to change their passwords regularly, may change their passwords between these times, and may only use passwords longer than a minimum length.

Recommendation

We recommend that the configuration of Novell be changed so that users are forced to change their passwords monthly, may change their passwords between these times, and may only use passwords of at least six characters.

4.8.3 Access Control over Regional Emergency Control System (RECS)

The RECS system on a VAX computer at Guildbourne House is commonly accessed remotely from Personal Computers (PCs) at Area Offices.

The access is controlled by a login script file on each PC which may be typed to the screen and inspected by the user. The login script file contains the telephone number of the modem, the password to the DEC Server, the username on the VAX computer and the associated password. The VAX username and password are the same and, because they are written into the login script for the PC, are never changed.

When access to the system is gained the user is taken immediately into the RECS system. However, users are able to interrupt the process just after their login and reach the operating system command line (the VMS $ prompt).

We understand that the supplier of the RECS program, Data Sciences, have been requested to change the program so that users are required to enter their username and password.

Recommendation

We recommend that the request that Data Sciences change the method of logging-in be pursued. We further recommend that following this modification users are issued with individual usernames and passwords, rather than district usernames and passwords, and which are not the same as each other.

4.8.4 Enforced Password Changes on VAX Systems

The Region operated two VAX computers at the time of the review. SRV01 ran the RECS system and SRV02 ran Charging for Discharges. The permitted lifetime of passwords on the two systems was reviewed.

On the SRV01 system most users have passwords which they are not forced to change. This is due to the operation of the RECS application which has been described in 4.8.3.

On the SRV02 system the majority of users with system privileges had a password lifetime of 30 days, and users without system privileges had a password lifetime of 90 days. This complies with the recommendations of the manufacturer of the VAX system, Digital. Three users with system privileges did, however, have password lifetimes of 90 days.

Recommendation

For the SRV01 system we recommend that following the assignment of individual usernames to users (see 4.8.3) password lifetimes be set to 30 days for privileged users and 90 days for non-privileged users.

For the SRV02 system we recommend that the three privileged accounts with password lifetimes of 90 days have this period reduced to 30 days.

4.8.5 Unused Accounts on the VAX Systems

The SRV01 and SRV02 systems were reviewed to determine if any accounts were present for which users had not logged-in for more than six months.

A significant number of accounts were identified on each of the systems where the user had not used the account for a period of more than six months, or where the user had never used the account.

Unused accounts represent a weakness in the controls over access to the computer systems. They are resources to which unauthorized access may be repeatedly attempted, or actually achieved, without detection.

Recommendation

We recommend that user accounts which are not used for a significant period be "disusered". A significant period may be one month for an account with system privileges and three months for a non-privileged account.

4.9 Staffing Issues

4.9.1 Independence of Quality Assurance Controller

The Region has appointed a Quality Assurance (QA) Controller. This post reports to the IS Manager.

The remit of the QA Controller includes the preparation of a QA Policy, QA Standards and Local Work Instructions for the IS Department. It is intended that the QA Controller will audit the work of the department as measured against these standards.

We understand that the QA Controller is expected to extend the scope of his work outside the IS Department.

In order that audit work may be effective it is necessary that the auditor be independent of staff directly responsible for the areas being audited.

Recommendation

We recommend that the post of QA Controller report outside any function for which it has audit responsibility.

4.10 Legality of Software Copies

The control of software licences appeared good. Some applications on PCs are network versions and have unlimited or controlled numbers of concurrent users.

4.11 Sensitive Applications

No findings additional to those detailed above have been made.

APPENDIX A

AUDIT REPORT NO: SN/004 LIST OF RECOMMENDATIONS

REC NO	PARA-GRAPH NUMBER	RECOMMENDATIONS	ACTION BY REGION	OFFICER RESPONS-IBLE	TARGET DATE FOR IMPLE-MENTATION
1.	4.2.1	We recommend that consideration be given to replacing the locks on the doors to the Computer Room by a swipe card lock system and that the doors be fitted with a self closing mechanism.	We will include this in an overall review of regional security which we will be conducting. In the interim the computer room doors have been strengthened and self closing locks installed.	Admin Manager	30 Jun 1993
2.	4.2.2	We recommend that access to the Computer Room be restricted to only those members of operations staff who require access to perform their duties.	Agreed	I.S. Manager	31 Mar 1993
3.	4.2.3	We recommend that access to computer equipment be restricted to computer operations staff. To this end we recommend that the equipment be housed separately from printers to which users have access and, if possible, from communications equipment.	Agreed. We are in the process of obtaining separate accommodation for use as storage, enabling existing accommodation to be released to house printing equipment.	Estates Officer	30 Sep 1993

AUDIT REPORT NO: SN/004 LIST OF RECOMMENDATIONS

REC NO	PARA-GRAPH NUMBER	RECOMMENDATIONS	ACTION BY REGION	OFFICER RESPONS-IBLE	TARGET DATE FOR IMPLE-MENTATION
4.	4.2.4	We recommend that consideration be given to replacing the keypad lock system for access to Guildbourne House with a swipe card lock system. This would have the additional benefit of enabling sensitive areas within the building, such as the computer areas, to be easily further secured.	The security review referred to in our response to Recommendation 1 includes a review of the security of Guildbourne House. The review is considering the use of the MicroTime card based time recording and access system. The Regional Management Team agreed this in principle in January 1993.	Regional Admin Manager	30 Jun 1993
5.	4.2.5	We recommend that a hand held fire extinguisher be placed in the Computer Room immediately.	Agreed. We will soon have two computer rooms which we will equip with hand held Halon extinguishers.	I.S. Manager	31 Mar 1993
		We further recommend that a thorough review of the fire detection and fire fighting requirements of the computer areas at each site be undertaken. This should involve equipment for the detection and automatic fighting of fires within the rooms and within the floor and ceiling voids. Consideration should be given to the fire resistant properties of the rooms themselves.	We have performed an initial risk analysis of critical systems in the Region. On the basis of this we have made a bid for funds to address our requirements in the 93/94 Corporate Plan. We will update our analysis in detail. This may be influenced by possible office changes in the Region following regional restructuring.	I.S. Manager	Already performed.

APPENDIX A

AUDIT REPORT NO: SN/004 LIST OF RECOMMENDATIONS

REC NO	PARA-GRAPH NUMBER	RECOMMENDATIONS	ACTION BY REGION	OFFICER RESPONS-IBLE	TARGET DATE FOR IMPLE-MENTATION
6.	4.2.6	We recommend that, should the siting of the Computer Room be reviewed at a future time, consideration of the risk of flood should be made in selecting a new site.	Agreed. We have surveyed the threat to the existing computer room and the cost of moving all of the computer equipment. This proved prohibitively expensive. We have moved some pipes in the kitchen so that they no longer lie over the computer room. We are also installing damp detection alarms in the ceiling and floor voids of the old and new computer rooms.	I.S. Manager	Already actioned.
7.	4.2.7	We recommend that a temperature sensor be installed in the Computer Room together with an alarm which will sound when the temperature exceeds preset tolerance limits. The alarm should sound in the continuously manned Control Room.	Agreed	I.S. Manager	Already actioned.
8.	4.2.8	We recommend that an EPO be installed in the Computer Room close to the door. The EPO should be easily reached from the doorway but not positioned so that it may be activated accidentally.	Agreed.	Technical Services Engineer	30 Apr 1993

AUDIT REPORT NO: SN/004 LIST OF RECOMMENDATIONS

REC NO	PARA-GRAPH NUMBER	RECOMMENDATIONS	ACTION BY REGION	OFFICER RESPONS-IBLE	TARGET DATE FOR IMPLE-MENTATION
9.	4.3.1	We recommend that development staff have no access to the live environment. Rather, transfers of code to a live area should be performed by operations, or a Database Administrator with no development responsibilities, following authorization. We understand that a new post of Database Administrator has been approved. This post will report to the Operations Controller. The recommendation would be satisfied by limiting the access to the live environment to the Operations Controller and his staff.	Agreed. This will be actioned following appointment of the DBA. This appointment has been delayed due to the job evaluation process.	I.S. Manager	31 Jul 1993
10.	4.4.1	We recommend that a form of off-site storage be implemented. This store should contain at least one recent backup of all files of the system at all times.	Agreed. We have implemented an interim procedure whereby operations staff take back-ups home at night. We will implement permanent arrangements when we occupy Wicker House, overspill office accommodation close to Guildbourne House.	I.S. Manager	30 Apr 1993

APPENDIX A

AUDIT REPORT NO: SN/004 LIST OF RECOMMENDATIONS

REC NO	PARA-GRAPH NUMBER	RECOMMENDATIONS	ACTION BY REGION	OFFICER RESPONS-IBLE	TARGET DATE FOR IMPLE-MENTATION
11.	4.4.2	We recommend that an operations procedures manual be drawn up to cover all of the systems running at the Region. In doing this we recognise that significant informal material which is already present will be incorporated in the manual.	Agreed in principle. We will implement this recommendation when staff resources become available.	I.S. Manager	31 Nov 1993
12.	4.6.1	We recommend that a formal agreement be entered into with a third party to maintain the UPS equipment. For ease of administration this could be drawn up following the installation of the new UPS equipment, provided that this does not result in undue delay in providing formal maintenance cover for the existing equipment.	Agreed.	Technical Services Engineer	Already actioned.

APPENDIX A

AUDIT REPORT NO: SN/004 LIST OF RECOMMENDATIONS

REC NO	PARA-GRAPH NUMBER	RECOMMENDATIONS	ACTION BY REGION	OFFICER RESPONS-IBLE	TARGET DATE FOR IMPLE-MENTATION
13.	4.7.1	We recommend that incoming modems are secured by the use of a dial-back device.	Agreed in principle. We will implement this recommendation when staff resources become available. We anticipate that we can complete the implementation by June.	Operations Controller	30 Jun 1993
14.	4.8.1	We recommend that the system for notification of leavers from personnel to IS and hence to IT Southern be revised so that users are removed from systems at the end of the day when they leave the NRA.	Agreed.	I.S. Manager	Already implemented.
		We further recommend that monthly comparisons of the mainframe user list and establishment list be conducted so that management can gain assurance that no non-NRA staff have access to the system.	We believe that a quarterly comparison will give sufficient assurance given the procedure we have agreed above.	I.S. Manager	Already implemented.
15.	4.8.2	We recommend that the configuration of Novell be changed so that users are forced to change their passwords monthly, may change their passwords between these times, and may only use passwords of at least six characters.	We have piloted the implementation of this recommendation. We will fully implement it by April.	PC Support Controller	30 Apr 1993

AUDIT REPORT NO: SN/004 LIST OF RECOMMENDATIONS

REC NO	PARA-GRAPH NUMBER	RECOMMENDATIONS	ACTION BY REGION	OFFICER RESPONS-IBLE	TARGET DATE FOR IMPLE-MENTATION
16.	4.8.3	We recommend that the request that Data Sciences change the method of logging-in be pursued. We further recommend that following this modification users are issued with individual usernames and passwords, rather than district usernames and passwords, and which are not the same as each other.	Agreed. We will implement the recommendation when staff become available. We anticipate that we will be able to complete implementation by August.	Operations Controller	31 Aug 1993
17.	4.8.4	For the SRV01 system we recommend that following the assignment of individual usernames to users (see 4.8.3) password lifetimes be set to 30 days for privileged users and 90 days for non-privileged users. For the SRV02 system we recommend that the three privileged accounts with password lifetimes of 90 days have this period reduced to 30 days.	Agreed. We will implement the recommendation when staff become available. We anticipate that we will be able to complete implementation by August.	Operations Controller	31 Aug 1993
18.	4.8.5	We recommend that user accounts which are not used for a significant period be "disusered". A significant period may be one month for an account with system privileges and three months for a non-privileged account.	Agreed. We will implement the recommendation when staff become available. We anticipate that we will be able to complete implementation by August.	Operations Controller	31 Aug 1993

AUDIT REPORT NO: SN/004 LIST OF RECOMMENDATIONS

REC NO	PARA-GRAPH NUMBER	RECOMMENDATIONS	ACTION BY REGION	OFFICER RESPONS-IBLE	TARGET DATE FOR IMPLE-MENTATION
19.	4.9.1	We recommend that the post of QA Controller report outside any function for which it has audit responsibility.	The role of the QA Controller will be restricted to the IS aspects of the Region's operations. It is, therefore, appropriate that in his audit role he report to the Regional ISSG.	Regional ISSG	30 Apr 1993, as procedures are developed.

W O R K I N G W I T H Y O U

Design: Laura Jane Valentine-Slack