Report of the Auditor-General

Auditor-General's Department

Report 7 of 2022

Review of system authentication

Government of South Australia

[P.P.4F

Report of the Auditor-General

Report 7 of 2022

Review of system authentication

Delivered to the President of the Legislative Council and the Speaker of the House of Assembly on 14 September 2022 and published on 16 September 2022 under section 38(2)of the Public Finance and Audit Act 1987

First Session, Fifty-Fifth Parliament

By authority: C. McArdle, Government Printer, South Australia

2022

The Auditor-General's Department acknowledges and respects Aboriginal people as the State's first people and nations, and recognises Aboriginal people as traditional owners and occupants of South Australian land and waters.

Auditor-General's
Department

www.audit.sa.gov.au

Enquiries about this report should be directed to:

Auditor-General
Auditor-General's Department
Level 9, 200 Victoria Square
Adelaide SA 5000

ISSN 0815-9157

Government of South Australia
Auditor-General's Department

Level 9
State Administration Centre
200 Victoria Square
Adelaide SA 5000
Tel +618 8226 9640
Fax +618 8226 9688
ABN 53 327 061 410
audgensa@audit.sa.gov.au
www.audit.sa.gov.au

14 September 2022

President
Legislative Council
Parliament House
ADELAIDE SA 5000

Speaker
House of Assembly
Parliament House
ADELAIDE SA 5000

Dear President and Speaker

Report of the Auditor-General: Report 7 of 2022 *Review of system authentication*

As required by the *Public Finance and Audit Act 1987*, I present to each of you this Report.

Content of the report

Our objective was to review the authentication controls applied across SA Government agencies. Our review did not highlight any systemic or fundamental system authentication control issues for the seven agencies we tested. We did note that the strength of authentication controls applied, including governance and password configuration settings, varied across these agencies and there were recommended areas of improvement.

Acknowledgements

The audit team for this Report was Andrew Corrigan and Tyson Hancock.

We appreciate the cooperation and assistance given by staff of the agencies entities we reviewed.

Yours sincerely

Andrew Richardson
Auditor-General

Contents

1 Executive summary

1.1 Introduction

Cyber security is high on the risk agenda of SA Government agencies and therefore must be effectively managed. To protect government services and sensitive information, agencies need to establish and maintain cyber security controls that meet the South Australian Cyber Security Framework (SACSF).[1]

A fundamental component of the SACSF is the need for robust authentication controls. Passwords are the most common authentication method. Effective authentication controls, including the use of strong passwords, help to validate a user's identity when accessing agency systems and prevent access by unauthorised individuals or attackers.

Agencies need to apply authentication controls to protect their systems, applications and information. They use Active Directory to authenticate users to their network, giving employees access to their file storage, print servers and business applications. Additional authentication controls might be implemented to access other resources.

Depending on their SACSF tier level,[2] agencies should, where possible, establish multi-factor authentication controls for any access considered to be higher risk (such as remote access, privileged access or access to external cloud-based solutions).

We reviewed the authentication controls applied across the SA Government. To do this, we selected a sample of seven agencies and reviewed the system authentication governance and controls they applied to their Active Directory domains and selected applications. We also performed a password cracking exercise to identify indicators of poor user password management behaviour.

We conducted our testing from March to May 2022.

1.2 Conclusion

Our review did not highlight any systemic or fundamental system authentication control issues for the seven agencies we tested. We did note that the strength of authentication controls applied, including governance and password configuration settings, varied across these agencies and there were recommended areas of improvement.

All agencies needed to better define and document the password settings they apply to their Active Directory environments and other business applications. In doing so, they should more fully adopt the guidance available to meet the requirements of the SACSF.

---

[1] The SACSF is a risk-based framework developed by the Department of the Premier and Cabinet. It aims to help agencies preserve the confidentiality, integrity and availability of their information by applying appropriate cyber security management processes. It is a mandatory framework for SA Government agencies.

[2] Agencies are required to select a tier level based on their risk profile, size, complexity and criticality of their organisation. The SACSF tiering model sets out the types of security controls that could be considered to address their policy requirements at each tier level.

To varying degrees, the Active Directory and application password settings we tested did not align with our recommended baseline settings. We identified weaknesses in user password behaviours, with several commonalties and trends occurring.

Although some agencies have implemented mitigating controls, they will need to consider their ongoing approach to ensure user passwords are strong and more difficult for an attacker to crack. This will help to maintain the security of agency systems and data.

1.3 What we found

Our key findings for the seven agencies we tested are summarised below. More details are provided in sections 4 and 5.

Gaps in documented password policies (section 4.1.1)

We found that agencies had not adequately defined and documented all password configuration settings in their IT policies.

Weaknesses in authentication controls (section 5.1.1)

We found, to varying degrees, that password settings for Active Directory and the selected applications we tested did not align with our recommended baseline settings.

Several agencies had Fine-Grained Password Policies[3] that did not align with our recommended baseline settings or that needed further review or documenting.

Several agencies had not applied multi-factor authentication to applications we tested. They were either not sure that it could be applied or advised us that they needed to further investigate it.

One agency needed to further investigate to determine the security controls used to store user passwords for an application we tested, while another two agencies were using a method that we thought was inadequate.

Several agencies advised us that they had mitigating controls to reduce the risks we identified. These included multi-factor authentication to access certain agency services, restricting the use of privileged accounts and machines, restrictions on workstation login attempts and alerting of potentially leaked credentials on non-SA Government systems.

In addition, some agencies' password configuration settings are administered on their behalf by the Department of the Premier and Cabinet (DPC), which manages the State Active Directory environment. These agencies would need to liaise with DPC when considering password controls to be applied and their risk appetite.

[3] Fine-Grained Password Policies allow different password policies to be applied to specific users or groups.

Weaknesses in user passwords (section 5.1.2)

We were able to crack many agencies' Active Directory account passwords within a short period of time.

We identified several common poor user password practices that needed to be addressed. They included the same password being used by more than one user, passwords containing common phrases, first or last names and passwords using similar formats. Other less common poor practices included the use of South Australian location, date, time and calendar words.

We did note that some of the accounts we tested were disabled. A compromised disabled account would not be able to access network resources and the weak passwords used may have been set before current password configuration settings were implemented. However, testing both active and disabled accounts helped us to better understand the types of passwords being used and the current and historical security culture of the agency.

We acknowledge that our password cracking exercise did not factor in other security controls that can reduce unauthorised access by an attacker, such as limiting authentication access to systems residing on the agency's internal physical network.

Inadequate management of shared privileged accounts (section 5.1.3)

Two agencies of the seven agencies we tested had privileged accounts that were being used by multiple IT personnel and one of them did not securely manage these credentials.

Neither of these agencies routinely changed privileged account credentials when key personnel changed roles or left the agency. This was inconsistent with their IT policies.

1.4 What we recommended

We made the following recommendations to address our findings.

Gaps in documented password policies (section 4.1.1)

Agencies should strengthen the documented password policies that apply to their Active Directory domain and the applications we tested.

We also recommended that agencies consider aligning their policies to the guidance provided in the Federal Government's Information Security Manual (ISM),[4] or an equivalent guidance framework that complements the objectives of the SACSF.

[4] The Australian Cyber Security Centre produces the ISM. The purpose of the ISM is to outline a cyber security framework that organisations can apply, using their risk management framework, to protect their information and systems from cyber threats.

Weaknesses in authentication controls (section 5.1.1)

Agencies should consider configuring their Active Directory and other application password settings in line with our recommended baseline settings (see section 4.1.1). Agencies in the State Active Directory environment should liaise with DPC on this.

Agencies should periodically review their password configuration settings against current best practice.

We also made several agency-specific recommendations including:

- implementing the password-based authentication controls specified in one agency's adopted security framework
- investigating whether multi-factor authentication could be applied for some applications we tested
- consulting with the system vendor on unsupported password settings
- considering alternative sign-on techniques for some applications
- reviewing the method used to store user passwords.

Weaknesses in user passwords (section 5.1.2)

Agencies should continue or increase their employee cyber security awareness programs to encourage better password management behaviours. For most agencies, we recommended users consider using a password manager or vault, particularly for privileged users accounts.

Agencies should also consider conducting regular password cracking exercises across their environments to identify and address any weaknesses.

Some agencies should consider whether it is possible to block the use of common words or phrases in passwords. Some of them may need to liaise with DPC about this.

We also made some agency-specific recommendations, including the review of disabled accounts and their associated privileges and removing Active Directory privileges as part of the employee termination process.

Inadequate management of shared privileged accounts (section 5.1.3)

We recommended that two of the seven agencies we tested ensure that privileged users are assigned their own individual accounts. If shared accounts are required, the credentials should be stored in a secure password vault that logs user access to them.

In addition, shared privileged account passwords should be changed when key personnel change roles or leave the agency.

1.5 Response to our recommendations

Agencies generally responded positively to our findings and recommendations with details of remedial actions and ongoing authentication strategies.

One agency raised concerns with some aspects of our recommendations, including the perceived administrative overhead and robustness of other mitigating controls.

DPC also provided feedback about our recommended baseline authentication settings and advised us that overall they were reasonable. DPC also advised us that ultimately agencies would need to consider their individual risk profiles before determining their specific authentication requirements. The SACSF tiering model provides guidance and expectations to assist agencies, but it is not a mandatory checklist. Agencies should therefore consider the security of a system according to the confidentiality, integrity and availability of its data.

Subsequent to our review, DPC released a whole-of-government SACSF guideline on password management that provides additional guidance to agencies on recommended authentication controls.

2 Background

As cyber incidents become more prevalent and sophisticated, and more agency data is held by third parties (including external cloud environments), the need for agencies to define and implement robust authentication controls is increasingly important. Agencies are challenged to balance security and operational impacts when it comes to configuring authentication requirements and getting users to set passwords that are harder for an attacker to crack.

Most cyber security frameworks now recommend that user passwords be longer and more complex by using a mix of cases, numbers and special characters.

Implementing minimum authentication controls and regular user education can help to drive improved user behaviour. Where possible, agency authentication systems should check not only whether a new password meets password requirements but also whether it contains easily guessable things, such as the user's name or user ID. This results in stronger passwords and helps to educate users.

Passphrases are also becoming more common to make it easier for users.[5] As passphrases are generally easier to remember, they can improve user security behaviours. Users may be less likely to use poor practices, such as writing down their password or using an incremental password scheme where a value at the end of the password is increased every password change. We acknowledge that moving to a passphrase approach requires organisational change and may not be possible in all IT environments.

We also acknowledge that recommended authentication requirements can differ between recognised security frameworks, including whether a user should be using a passphrase or a password. Recommended settings are also being constantly reviewed and updated.

[5] A passphrase is a string of words known to the user but is longer and hence generally more difficult to crack than a password.

3 Review mandate, objective and scope

3.1 Our mandate

The Auditor-General has authority to conduct this review under section 36(1)(a)(iii) of the *Public Finance and Audit Act 1987.*

3.2 Our objective

Our objective was to review the authentication controls applied across SA Government agencies. We designed our testing to identify risks and vulnerabilities that could threaten the security of agency information systems and the data they contain.

3.3 What we reviewed and how

To conduct our testing, we selected a sample of small, medium and large SA Government agencies. We reviewed the following areas to determine if agencies had established appropriate authentication controls relating to Active Directory and selected applications:

- documented IT policies relating to user authentication, including requirements for passwords and the use of multi-factor and other forms of authentication
- the configuration of password controls
- the strength of user passwords.

Our testing involved:

- inspecting governance documentation
- inspecting implemented password configuration settings using walkthroughs and screenshots
- identifying default configurations
- assessing password policies
- assessing user account management processes and password storage methods
- performing a password cracking exercise.

The SACSF provides agencies with the flexibility to choose the way they address the 21 policy statements, to align with their own risk profiles. For consistency when reviewing multiple agencies, we based our review primarily on the requirements set by the ISM, which are accepted by the SACSF.[6]

[6] Detailed recommended security settings can differ between security frameworks.

3.4 What we did not review

Our review had a specific focus on system authentication controls applied by agencies.

As noted in section 3.3, for consistency we based our review primarily on the requirements set by the ISM. We did not perform any assessments against alternative security framework baselines accepted by the SACSF and adopted by some agencies. We acknowledge that these alternative security frameworks can be equally as effective as the ISM.

Some accounts we tested were disabled. We did not test the processes agencies used to remove privileges provisioned through Active Directory as part of the employee termination process.

Our password cracking exercise using a password cracking tool was designed specifically to test the strength of passwords used by agency users. Password cracking tools do not take into consideration other mitigating controls. The associated risk of weak passwords can be reduced by other security controls that help prevent unauthorised access by an attacker. Examples include account lockout controls to prevent brute-force password attacks, multi-factor authentication, security alerting and restricting access to password files stored in systems.

We did not conduct any validation testing on the use and security of password vaults.

4 Security governance

4.1 Detailed findings

4.1.1 Gaps in documented password policies

Recommendation

We recommended that agencies strengthen the documented password policies that apply to their Active Directory domain and the selected applications we tested.

We also recommended that agencies consider aligning their policies to the guidance provided in the ISM or an equivalent guidance framework that complements the objectives of the SACSF.

Finding

As previously stated, while the SACSF gives agencies the flexibility to choose the way they address the 21 policy statements, we based our review primarily on ISM standards. The ISM has two preferred approaches for password management. We performed our testing using the following baseline passphrase/password settings.

Figure 4.1: Our recommended baseline passphrase/password configuration settings[7]

Password setting	Passphrase-based approach	Password-based approach
Minimum password length	14 characters	10 characters
Maximum password age	90 days	
Minimum password age	1 day	
Complexity	Not enabled	Enabled
Account lockout duration	Standard account: 15 minutes (an administrator can unlock an account for use immediately) Privileged account: 0 minutes (unlock to be performed by an administrator)	
Account lockout threshold	5 invalid login attempts	
Multi-factor authentication[8]	Enabled for all external access to agency resources where possible (web applications, VPN, external file share). Also applicable for high-risk user accounts such as administrator accounts.[9]	
Successful and unsuccessful authentications are logged	Logging of failed and successful login attempts is enabled.	

[7] These are our recommended baseline settings at the time of our review, based on better practice guidance including, the SACSF and the ISM. We note that the ISM and its recommended settings are constantly reviewed and updated.

[8] Multi-factor authentication adds another layer of protection against compromise by requiring users to verify their identity by one or more factors in addition to their username and password.

[9] If multi-factor authentication is enabled the recommended password configuration settings, such as password length, are less onerous.

Our testing of the seven agencies we selected identified the following gaps in their documented password policies:

- the IT policy applicable to Active Directory for some agencies did not specify guidelines for certain password configuration settings
- the IT policies for some applications we tested did not specify password configuration settings that should be applied or reference any other guidance
- for one agency, the IT policy applicable to Active Directory and another application we tested had not been updated to reflect the password requirements of its adopted security framework.

Why this is important

Formally documented policies provide clear guidance to agency users about minimum password complexity requirements. They also help ensure that any new systems or services are configured with authentication controls that align with agency-wide password policy requirements.

5 Authentication security

5.1 Detailed findings

5.1.1 Weaknesses in authentication controls

Recommendation

We recommended that agencies consider configuring their Active Directory and other application password settings in line with our recommended baseline settings (see figure 4.1) or an equivalent guidance framework that complements the objectives of the SACSF. This includes any Fine-Grained Password Policies. Some agencies may need to liaise with DPC to implement these recommendations.

Agencies should also periodically review their password configuration settings against current best practice.

We also made the following agency-specific recommendations for the seven agencies we tested:

- for one agency, we recommended ensuring that it has formally risk assessed and implemented all the accepted password-based authentication controls listed in its adopted security framework
- for four agencies, we recommended investigating whether multi-factor authentication can be applied to the selected applications we tested
- for one agency, we recommended the agency consult with the system vendor of a legacy application.[10] This was to clarify whether the unsupported password settings could be configured or whether an alternative sign-on technique could be adopted
- for another agency we also recommended they consider alterative sign-on techniques for the selected applications we tested
- for three agencies, we recommended reviewing the security method that had been applied to store user passwords.

Finding

Agencies use Active Directory to authenticate users to their network. This allows employees to access their file storage, print servers and some business applications. Other applications may require a separate user sign-on.

Our testing identified that:

- to varying degrees, password settings for Active Directory and the selected applications we tested did not align with our recommended baseline settings

[10] A legacy ICT system is an outdated system that is either unable to be upgraded, in need of modernisation (eg to interface with other business systems) and/or no longer supported by the vendor, including security updates, or support is limited.

- several agencies had Fine-Grained Password Policies that did not align with our recommended baseline settings or that needed further review or documenting
- for four agencies, multi-factor authentication was not applied to the applications we tested. In some instances, agencies were not aware if it could be applied or needed to further investigate it
- one agency needed to further investigate to determine the security controls used to store user passwords for an application we tested, while another two agencies were using a method that we thought was inadequate.

Several agencies advised us of their mitigating controls, including the use of multi-factor authentication when users access certain services. One agency noted that their workstations are also configured to restrict failed login attempts and alerts are received of potentially leaked credentials on other non-SA Government systems. Another agency advised us that it had implemented controls to restrict the use of its privileged accounts and machines.

Some agencies' password configuration settings are administered by DPC on their behalf. These agencies would need to consider the password controls applied and their risk appetite.

Why this is important

Weak password controls increase the risk of accounts being compromised and unauthorised access to agency systems, potentially resulting in data loss and access to sensitive information.

There are risks if the following password configuration settings are not appropriately defined:

- **Minimum password length:** Minimum length requirements are set to ensure passwords are long enough to better withstand password cracking activities, increasing the time it takes to crack them.
- **Maximum password age:** Specifies the maximum number of days a password can be used before it is required to be changed. Specifying a maximum password age prevents indefinite access if a password is compromised.
- **Minimum password age:** Specifies the minimum number of days a password can be used before it is required to be changed. Enforcing a password change reduces the likelihood that a user will attempt to immediately change to a previously used password.
- **Complexity:** Simpler passwords are easier to compromise through brute-force attacks. Enforcing the use of complex passwords using a mix of upper and lower-case letters, numbers and symbols makes it harder for an attacker to crack them.
- **Account lockout duration:** An appropriately long lockout duration is required to reduce the number of attempts a malicious user has at guessing a password over a period. Given privileged accounts have a heightened level of access to alter user access profiles and make system changes, they should be manually reset by an administrator.
- **Account lockout threshold:** The number of incorrect password attempts allowed before an account is locked out. Allowing too many incorrect password attempts increases the risk of an account being compromised, such as through a password cracking tool.

- **Successful and unsuccessful authentications are logged:** Enabling account authentication audit logs allows monitoring and detection of any signs of account compromise or brute-force attempts and helps incident analysis.
- **Multi-factor authentication:** Adds another layer of protection against compromised accounts by requiring users to verify their identity by one or more factors in addition to their username and password.
- **Store passwords securely:** Applying secure password storage methods reduces the likelihood of credentials being exposed to potential compromise. This, coupled with strong password parameters, significantly extends the effort required to compromise account credentials.

5.1.2 Weaknesses in user passwords

Recommendation

We recommended that agencies continue or increase their employee cyber security awareness through periodic newsletters or communications to encourage better password management behaviours. For most agencies, we recommended users consider using a password manager or vault, particularly for privileged users.

We also recommended that agencies consider conducting regular password cracking exercises across their environments to identify indicators of poor user password management behaviour.

For some agencies, we recommended investigating whether it is possible to implement a 'disallow' list of common words or phrases within the identity authentication provider.[11] Some agencies should liaise with DPC about this.

We also made the following agency-specific recommendations:

- one agency should review its disabled accounts to ensure that any assigned privileges were removed
- two agencies remove user Active Directory privileges as part of the employee termination process.

Finding

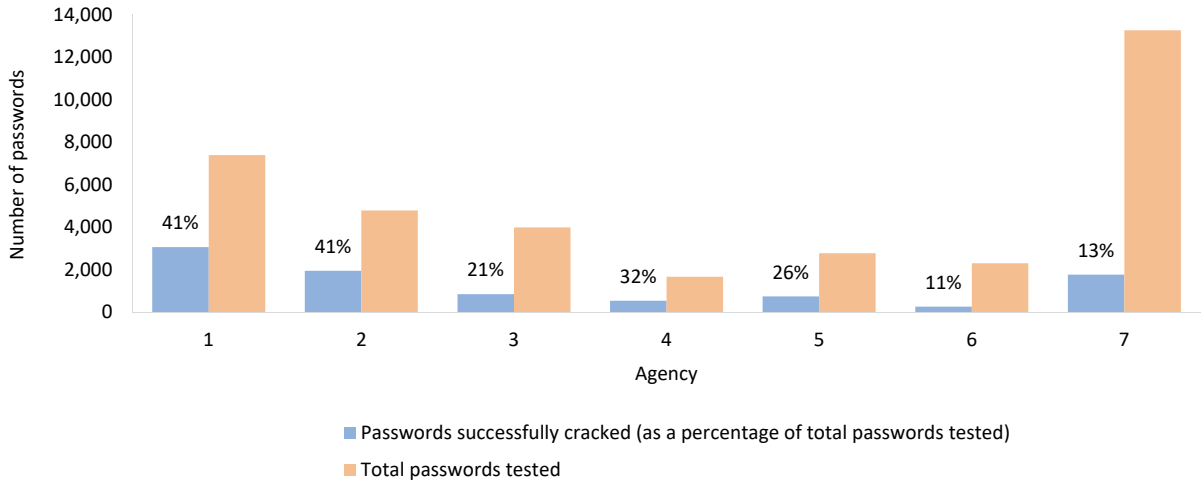
We conducted a password cracking exercise across each agency's Active Directory environment and were able to crack many passwords within a short period of time. We considered these passwords to be weak, with many of them commonly used and expected by attackers when performing equivalent password cracking exercises.[12]

[11] A system that manages user identity information and provides authentication services.

[12] Wordlists are publicly available and contain a collection of commonly used passwords, which attackers use to aid password cracking techniques.

It should be noted that using an automated password cracking tool does not take into consideration other mitigating controls that could minimise the overall risk to the agency. Examples include account lockout controls to prevent brute-force password attacks, multi-factor authentication, security alerting and restricting access to password files stored in systems. We did not test whether all these controls exist and their potential effectiveness. Instead, the overall purpose of our password cracking exercise was to identify indicators of poor user password management behaviour.

Figure 5.1: Summary of password cracking results

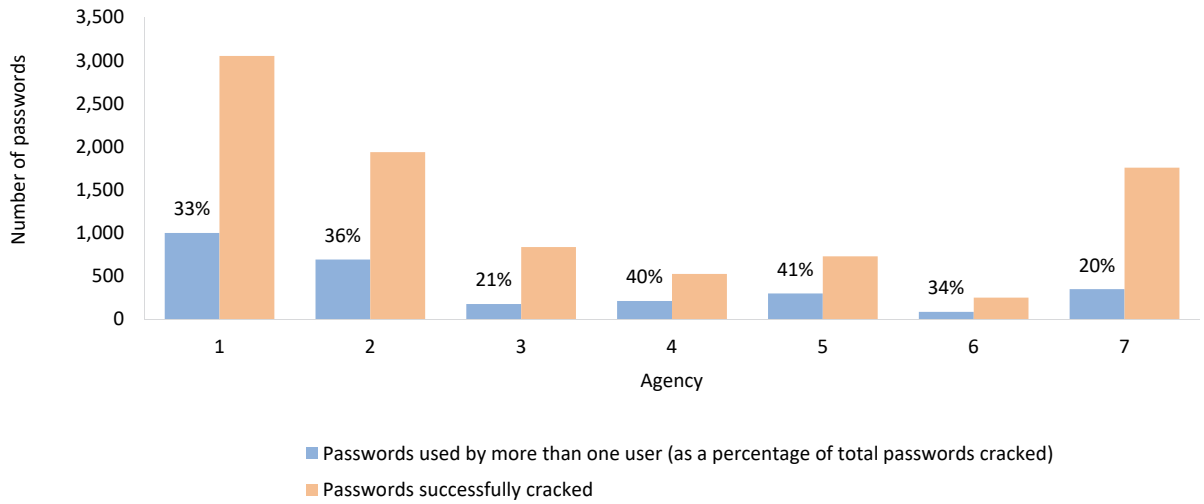


We tested both active and disabled accounts. In figure 5.1, Agency 1 and Agency 7 included many disabled accounts. Weak passwords may have been set on disabled accounts before the agency's current password configuration settings were implemented.

Agency processes for removing Active Directory accounts that were no longer required and their associated privileges varied between agencies.

On average, 32% of the passwords we successfully cracked were used by more than one user.

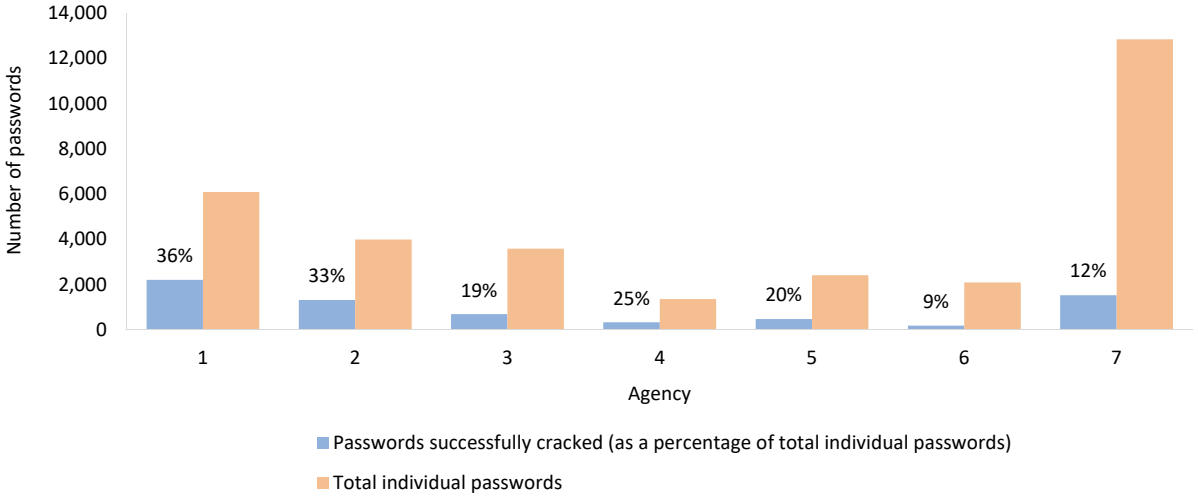
Figure 5.2: Passwords used by more than one user



We also identified the number of individual passwords.[13] We were able to crack an average of 22% of individual passwords across the agencies we tested. The use of weak passwords may be due to:

- users not being aware of the importance of creating strong individual passwords or not following guidance provided in the agency's security policy
- a lack of availability or awareness of password managers or vaults that make it easier for users to set stronger passwords.

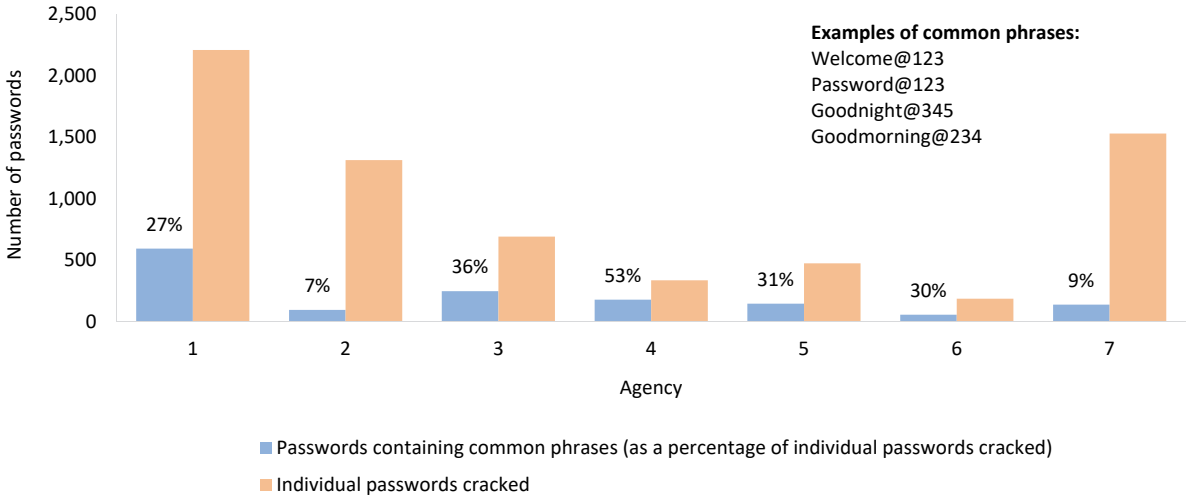
Figure 5.3: Individual passwords identified and cracked



Our testing identified several trends in agency Active Directory domains.

Several of the individual passwords we cracked contained a common phrase, such as an English greeting.

Figure 5.4: Passwords containing common phrases



[13] Individual passwords were determined based on the number of unique (individual) hashes.

We also identified that individual passwords we cracked at some agencies contained a South Australian location, such as a suburb or city name.

Examples of common locations include:

- Adelaide5000
- Mitcham5062
- SouthAustralia@123
- Adelaide@123.

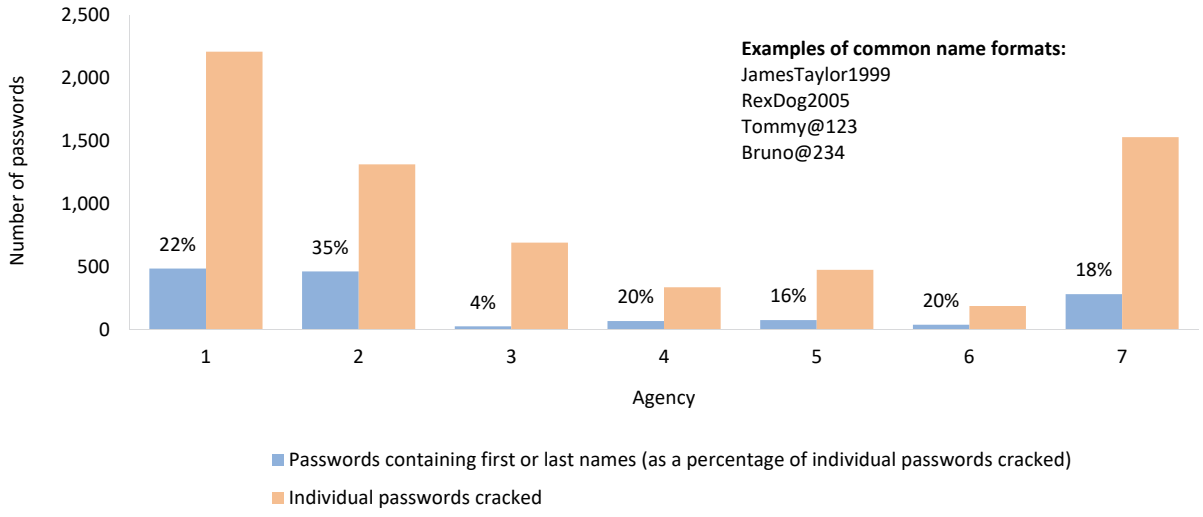
For two agencies, we noted that an average of 19% of the individual passwords we cracked contained date, time or calendar words, such as days of the week, months or seasons.

Examples of common date, time or calendar words include:

- June2022
- Spring2021
- 12July1999
- 26January2022.

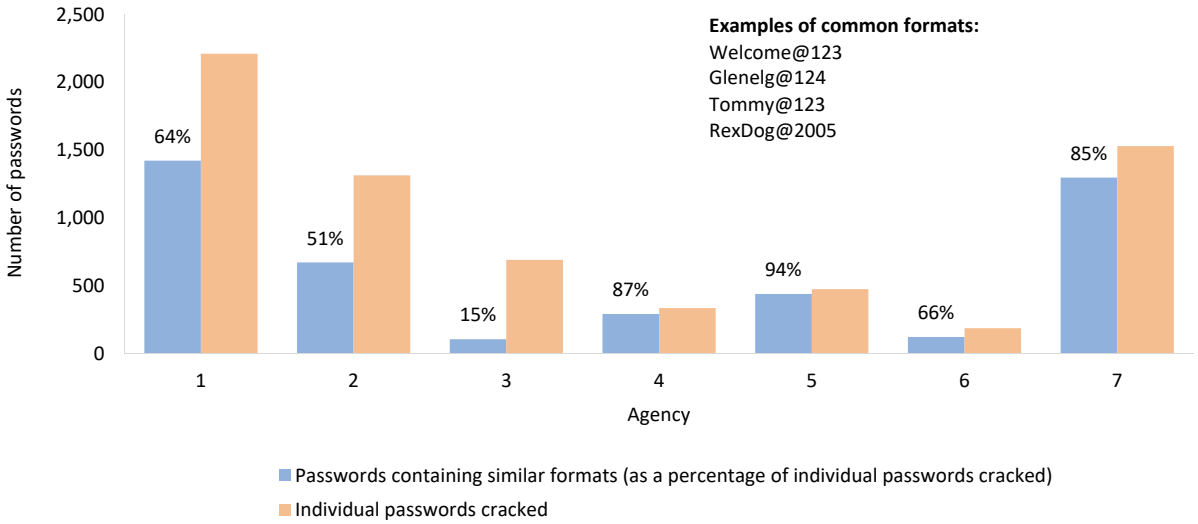
Many individual passwords we cracked contained a person's name (either the user's or another person's), such as their first or last name, in varying combinations. We note that two agencies had implemented a control to prohibit the use of the user's name or user ID.

Figure 5.5: Passwords containing first or last names



In addition, we found that many of the individual passwords we cracked followed a similar format. For example, the first letter was often capitalised and the final characters were a mix of numbers and special characters.

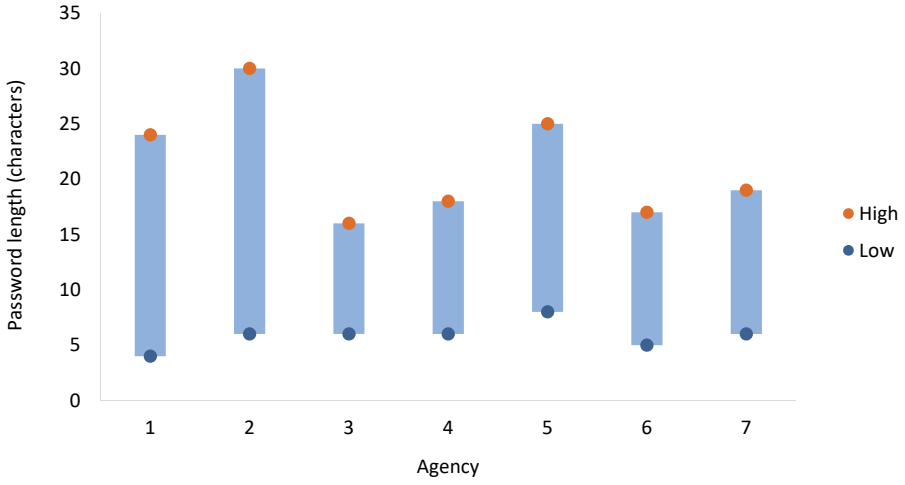
Figure 5.6: Passwords containing similar formats



Password lengths varied from four to 30 characters across the agencies we tested. The most common password lengths are shown in figure 5.8.

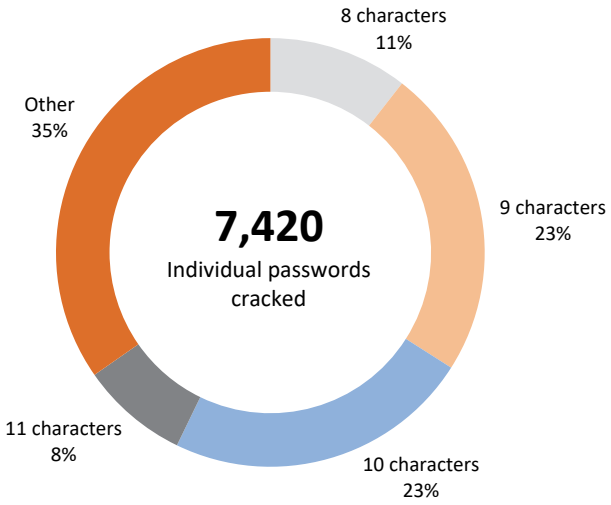
We note that the passwords we tested included disabled accounts. In these instances, we acknowledge that some passwords may have been configured before the agency's current password settings were established.

Figure 5.7: Highest and lowest password lengths



Of the total individual passwords we cracked, the most common password length was between eight and 11 characters.

Figure 5.8: Most common password lengths



Some of the individual passwords we cracked had a shorter length than the agency's current setting for minimum password length. Reasons include:

- disabled accounts having been set with short passwords before the agency's current password policy was configured
- administrators having exclusively set accounts with short passwords, bypassing the current password policy. There may have been instances where this was required, for example because a legacy application or system does not support longer passwords.

Why this is important

Using weak passwords weakens the overall security posture of the Active Directory environment and the business applications that rely on Active Directory for authentication and authorisation.

Strong password rules, such as requiring a mix of character types, improve the uniqueness of passwords. Users need to create passwords that are difficult for an attacker to compromise (ie not commonly used or easily identifiable information).

5.1.3 Inadequate management of shared privileged accounts

Recommendation

For accountability purposes, we recommended that two agencies ensure that privileged users are assigned their own individual accounts. If shared accounts are required, the credentials should be stored in a secure password vault that logs user access to them.

We recommend that shared privileged account passwords be changed when key personnel change roles or leave the agency.

Finding

For two agencies, we found that the password for a single privileged account is being shared among multiple support personnel. One of these agencies did not securely manage the credentials.

At both agencies, we identified that shared privileged account passwords are often not changed when key personnel change roles or leave the agency.

These practices were inconsistent with the agencies' policies.

Why this is important

Using shared accounts reduces individual accountability and the traceability of actions performed through these accounts. In addition, shared account credentials are often not changed regularly, increasing the risk of the accounts being used inappropriately by users that have changed roles or been terminated.

Appendix – Glossary of abbreviations and terms

Term	Description
Active Directory	Used to authenticate users to the network. This allows users to access file storage, print servers and business applications.
Australian Cyber Security Centre	Leads the Australian Government's efforts to improve cyber security. For more information refer to https://www.cyber.gov.au.
Department of the Premier and Cabinet (DPC)	The lead agency supporting the Premier and Cabinet by developing policy and delivering programs to realise the SA Government's vision for South Australia.
Fine-Grained Password Policies	Allow different password policies to be applied to specific users or groups.
Identity authentication provider	A system that manages user identity information and provides authentication services.
Information Security Manual (ISM)	The Australian Cyber Security Centre produces the ISM. The purpose of the ISM is to outline a cyber security framework that organisations can apply, using their risk management framework, to protect their information and systems from cyber threats.
Legacy ICT system	An outdated system that is either unable to be upgraded, in need of modernisation (eg it is unable to be interfaced with other business systems) and/or no longer supported by the vendor, including security updates, or support is limited.
Multi-factor authentication	Adds another layer of protection against compromised account by requiring users to verify their identity by at least two or more factors in addition to their username and password.
Passphrase	A string of words known to the user but longer and generally more difficult to crack.
Password hashing	The process of turning a user's password into a scrambled series of letters and/or numbers using an encryption algorithm.
South Australian Cyber Security Framework (SACSF)	A risk-based framework developed by the Department of the Premier and Cabinet. It is aimed to assist agencies with preserving the confidentiality, integrity and availability of their information by applying appropriate cyber security management processes. It is a mandatory framework for SA Government agencies.
State Active Directory Environment	Incorporates several, but not all, SA Government agency networks and Active Directory forests.
Virtual private network (VPN)	Created by establishing a virtual point-to-point connection via dedicated circuits or with tunnelling protocols over existing networks. Is used to extend a private network across a public network.
Wordlists	Contain a collection of commonly used passwords that attackers use to aid password cracking techniques.