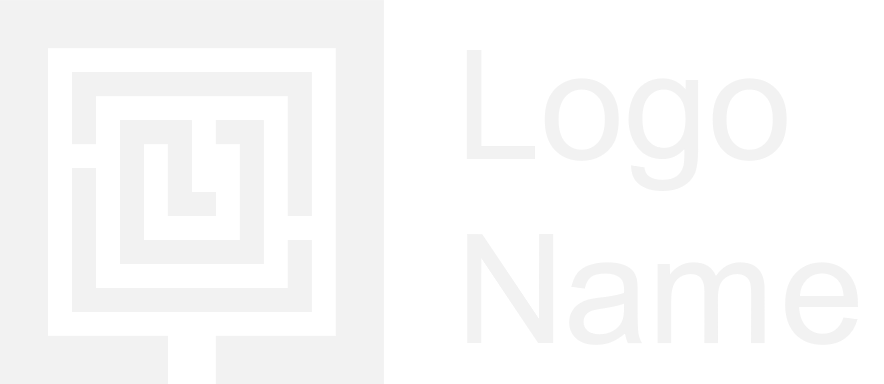
| text divider |
| --- |
|  |

colored rectangle

# Executive Summary

This is the executive summary. This should be 2-4 paragraphs that provides the high-level, non-technical overview of the report. It should include the background, very short summary of the activities, any critical findings, any conclusions or future work.

Also, the last paragraph should be a short “Thank you” to the individuals at the organization, or contractors, or whoever, that assisted with the assessment. Acknowledge their assistance – it always helps in the future.

questions and key points:

after finishing the report come back to summarize it. (makes more sense to write about something you know)

Who are the individuals at the organization, or contractors, or whoever, that assisted with the assessment? ….. DSC? NARO inc.?

Contents

[1](#_gjdgxs) Executive Summary 2

[1](#_30j0zll) Introduction 4

[1.1](#_1fob9te) Background 4

[1.2](#_3znysh7) Scope 4

[1.3](#_2et92p0) Report Organization 4

[2](#_tyjcwt) System Overview 5

[2.1](#_3dy6vkm) Facility or System 1 5

[2.2](#_1t3h5sf) Facility or System 2 5

[2.3](#_4d34og8) Facility or System 3 5

[3](#_2s8eyo1) Assessment Methodology 6

[4](#_17dp8vu) Assessment Activities 7

[4.1](#_3rdcrjn) NARO Documentation Review 7

[4.2](#_26in1rg) In-person Interviews 7

[5](#_lnxbz9) Assessment Results and Recommendations 8

[5.1](#_35nkun2) Weaknesses 8

[5.2](#_1ksv4uv) Strengths 9

[5.3](#_44sinio) Observations 9

[6](#_2jxsxqh) Conclusions and Follow-on Activities 10

# Introduction

Quick introduction to this section. This section includes…

## Background

Why is this assessment happening? For example:

The reason for this assessment is the recent ransomware attack suffered by ANRO. This resulted in NARO becoming more serious about their cybersecurity efforts. At the time of conducting the assessment, all of NARO security and computer related tasks are managed by their “IT guy” Henry. Since Henry works with another business along with NARO they realize they are limited to what services the business can request and when they can be requested.

## Scope

*What was in-scope for this assessment, what was out-of-scope for this assessment, and things looked at. This includes any limitations to the assessment. In a hands-on assessment, production systems might be out-of-bounds, so this would be mentioned here.*

In-scope:

* password security measures
* backup methods
* physical security
* server room
* employee laptop handling
* servers
* company software
* company hardware

out-of-bounds:

* requesting details about tokens or information related to third party servers
* credit card processing security
* access logs
* real estate records

## Report Organization

The rest of this report is organized as follows: Section 2 provides an overview of the NARO facilities, systems, and processes used. Sections 3 and 4 describe the methodology used by the team and the activities they conducted. The assessment results are found in Section 5, with conclusions and recommended follow-on activities in Section 6. Appendices include additional information related to the assessment.

# System Overview

The introduction to this section should have 1-2 paragraphs about the overall system. It’s overall purpose, facilities, etc.

* facilities
  + office
  + workstations
  + remote
  + computer closet

The NARO is a company that consists of a main facility (the office), workstations, a storage closet and company network (remote work). The main office is where the majority of company business takes place. Individuals can enter this office between the hours of 6am and 10pm on business days. Inside the office there are a total of 20 workstations (one for each employee).

Employees will often work at these stations to connect to company server and software. Along with this NARO has a company network that can be accessed remotely using one of the 4 company laptops. The network is upheld by the storage closet aka the server room. The server room is unlocked at all times so anyone who has accessed to the main office has access to the server room.

## Facility or System 1

The first facility that was analyzed was the main office building. The NARO office is located on the 13th floor of a high rise in downtown San Antonio. The business neighbors a real estate development firm, oil and gas services firm and an empty office that was leased to an investment firm charged with fraud. The company has a one person IT department who currently works with another company along with NARO.

During the interview we noticed major vulnerabilities with the office and building authentication methods. Since there are no intercom systems, anyone with a proxy card can enter the NARO office space. They simply have to pass through the receptionist desk. It’s clear that this leaves the ability of individuals who are not authorized to enter the office. Furthermore the company is lacking in proper practices in terms of piggybacking awareness. When asked if the company was concerned with piggybacking they were unaware of the content of the term. There is currently no log to confirm who and who has not entered the office space. When a receptionist needs to let someone in they can simply do so with a press of a button. This becomes a concern because during the receptionist off hours it would be relatively easy for an unknown person to let themselves in the office space.

This is a description of the first system or facility. There are a variety of ways to organize this breakdown, and it will depend on what seems the best for each assessment – and the recipients of the report. For example, if you look at multiple types of systems at multiple facilities, it may depend on how the organization has their areas of responsibility. For example, at UTSA, if you were looking at the various IT systems deployed around campus, you might break it down by functionality – email, wireless access, etc. If you were looking at fire detection and suppression systems – smoke detectors, sprinklers, emergency alerts, fire extinguishers – it might make sense to break it down by buildings since they were constructed at different times and probably have different systems installed. Plus, some buildings may have special requirements (like storing chemicals) which a standard office building wouldn’t be worried about.

**Key items**:

* Staff consist of 20 full time employees
* Manager has their own office
* 3 accounting team members share an office
* there is one receptionist that works 9am - 5pm
* office is open from 6am - 10pm
* one space was formerly leased to an investment firm charged with fraud
* access to NARO office only requires building proxy card

**Key items**:

This should provide enough information that all of your findings can trace back to this section. That way, if information is incorrect, you can trace back to where it went wrong. Plus, in 5 years, the source information may be shredded and gone – and only this report is left to reference.

Also, this section should be factual and descriptive. This isn’t the section to say something is good/bad/whatever. Also, if you don’t KNOW something, but THINK it is a certain way – make sure you state that.

## Facility or System 2

The next system is the employee work stations. Each of the computers at the workstations are running windows operating systems. When employees leave their workstations their systems are left running and if they are using company software there isn’t an auto logout feature that triggers after a certain amount of inactivity. Employees do not use proper password safety methods. They sometimes write passwords down and leave it available for anyone to see on their desks. Employees are not required to change their passwords. They will go months without changing their passwords or checking if any of their passwords have been compromised. Employees leave important documents out on their desk when they are in and out of their stations.

**Key items**:

* Each employee has a workstation
* passwords are changed at various times (every 3 months or so)
* passwords information is left out on desks
* company information is left out on desks when not being utilized
* NARO software does not utilize auto logout technology

## Facility or System 3

The next system is the company’s network and servers. In order to connect to company servers outside of the office employees must use either their mobile devices or company laptops. The company servers are not enabling any firewalls or technical security methods. The only security they used is security built into their windows operating systems (windows defender). Since there are only 4 company laptops most employees utilize their personal devices to access information on the network. There are no known authentication methods other than putting in the employees usernames and passwords. All documents can be accessed using the office 365 site.

The NARO company utilizes 3 physical servers that are all located in the office storage room. The storage room is always left unlocked so their IT person Henry can access it during any time of the day. When Henry works in the server room he uses usb drives and other external devices to upload and download data from the servers. Everything is stored on the file server meaning that everything is accessible from one place on the server.

**Key items**:

* Company has 4 employee laptops
* Company can access server files through office 365 from their personal devices
* Company servers do not use firewalls
* NARO has 3 servers located in the storage room
* The storage room is always left unlocked
* usb and external devices are often connected to the physical servers

# Assessment Methodology

The **Information Technology Laboratory** at the National Institute of Standards and Technology promotes the U.S. economy and public welfare by providing technical leadership for the Nation’s measurement and standards infrastructure. 1 Information Technology Laboratory developed tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. Information Technology Laboratory’s responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in Federal information systems. ***This Security framework is based on NIST SP800-53 revision 5 and the NISTIR 7621 revision 1*** published by The Information Technology Laboratory, with the purpose of serving a concise yet robust and easy to understand security model for small business who may not have the expertise or understanding to answer many of the items found in detailed checklists, may not have a lot of time to dedicate to the process, or may not have the funding to bring in a 3rd party to conduct the audit.

(guerrero)

# Assessment Activities

The introduction should simply state that this section covers the high-level activities performed by the assessment team. It should also state that the observations and findings made from these activities are discussed in Section 5.

## NARO Documentation Review

* Least Privilege Users should only be allowed to use privileged software based on their role in the business. By limiting the amount of privilege that a user has access to, if, theoretically, the user’s account was compromised, it would limit the number of systems that are impacted and could be used for malicious purposes. Within the least privilege control, we could also employ enhancement 3 which includes authorizing network access commands for certain operational needs while also documenting the reasoning behind such needs.
* Concurrent Session Control: A small business should take care of how many concurrent sessions its employees have access to based on the role of the employee. By closely monitoring the attempts that an employee has made in having various sessions open, a small business can use this as a detection measure to see if high levels of attempts are caused by a compromised user, this also limits the attackers window of operation as it would be easy to trigger such a detection measure.
* Remote Access: As more and more employers have shifted to remote work, it can be deduced that an attacker will attempt to compromise a user’s account using the employee’s personal computer, as a personal device has less security than that of an enterprise device. We can further strengthen this control by implementing enhancement 10 (Authenticate remote commands) by implementing a two-factor authentication process that requires an employee to input a pin and a token so that specific commands and logins can be verified; this provides strong protection in assuring that an employee and not an attacker is the individual that is logging in.
* Access Control for Mobile Devices: Personal handheld devices are the most prevalent form of communication, and if an attacker was to compromise an employee’s mobile device, the attacker would have an array of sensors and tools that could be used to spy and further advance their attempts of intrusion. Implementing policies that limits mobile device usage can further enhance the security of a small business the rationale behind such policies is due to the possibility of employees not having the lates security patches updated to their mobile devices, such lack of patches can cause an attacker to exploit the employee’s mobile device and use it to compromise any system an employee connects their device to.
* 21 Information Sharing: Information sharing can be an easy oversight, if an employee has the privilege to send emails with sensitive information outside of the organization, this can cause huge regulatory issues, along with providing attackers the ability to send mass amounts of information outside of the business without raising suspicion. This can further be enhanced to include the restriction of external communication, only specified users can have access to send out external emails which would require that the emails sent out along with the users account have extra scrutiny in case the account is ever compromised.
* Policy and Procedure: This control falls under the category of awareness and training, and the purpose of such a control is to build policies that reduce the possibility of an attacker compromising a system or network. Management can create awareness information and develop training materials that users can learn upon.
* Literacy Training and Awareness: The purpose of such a control is to raise employee awareness of disguised cybersecurity threats. Human error is usually the biggest weakness, and for a small business, it can be easier to assure that most if not all employees are aware of the tactics used to compromise a network. By having quarterly training sessions and knowledge checks along with mock attack, the human error can be greatly reduced.

## In-person Interviews

-Isai

On whatever date, the team met with WHOEVER from NARO, Inc. to discuss…

# Assessment Results and Recommendations

Jasmine-

The intro to this section should discuss that the results obtained from the assessment activities in Section 4 are in this section. It should also mention that this section will include strengths, weaknesses, and observations.

Strengths are things they are doing well. This is to give them some good news to go with the bad news. Plus it makes sure they don’t stop doing those things as they mitigate the weaknesses.

Weaknesses are things that could be a vulnerability, or otherwise help out an attacker. For example, they could be running an older version of Windows, or outdated antivirus. Or, it could be something like the cleaning company has keys to the buildings, but has no idea who should be allowed in the building – so someone could gain unauthorized access. Also, weaknesses should have a severity rating. There are many different rating systems out there – from the simple, to the incredibly complex. (I have used one that required multiple spreadsheets to calculate the overall score based on CVSS scores and other inputs.) I recommend you use HIGH, MEDIUM (or MODERATE), and LOW to keep it simple.

Observations are things that are not strengths or weaknesses, or doesn’t have enough information to really make a determination. So, imagine it was a hands-on assessment, but you couldn’t touch the production systems since they are supporting critical business operations. If you notice that one of those systems is unlocked, and no one is around, it is probably bad – but it is out of scope, so you don’t call it a weakness. Because, for all you know, someone made the lock screen image look like the desktop as a joke.

Also, if you do this professionally – do NOT go outside of your rules of engagement and the scope of the assessment. It doesn’t matter how cool something looks, or seems like you could compromise a system in 5 minutes. (Also, never do work without a rules of engagement that has been signed by the cognizant authority.)

## Weaknesses

(3 per member)

**(High) Backups of critical systems and data has not been performed in over 2 years.**

Justification: A lack of backups means that systems can not be restored in the event of a ransomware attack or system failure. Manually entering the information from paper files would take approximately 3 months.

Mitigations: Create a backup procedure that is followed on a regular basis. This should include off-site storage of backups, encrypting the backups to ensure the data is secure when taken off-site, and regularly testing that the systems and databases can be restored from the backups.

NOTE: Each finding/weakness should have more detail, providing enough information to support your severity rating. In addition, the mitigation(s) should specifically address this issue. Keep each one “self-contained” where someone trying to fix a specific issue has all the information in the finding.

## Strengths

(1 per team member)

**Physical Security**:

* Only the facility manager, assistant manager, and CEO have keys to access the building and the code to disarm the alarm system.

**Backups**:

* Daily backups are stored on AWS, and a weekly backup is made using an Ironkey flash drive which is taken off-site to the company safe deposit box at a local bank branch. In addition, both procedures are conducted by two people who verify it was completed correctly, and report the successful backup by sending an email to the CEO.

## Observations

(1 per team member)

**Employees use their personal mobile devices to access work systems**

Description: Employees are able to use their personal devices to access work systems such as email, calendar, time reporting, and most work functions. However, it was unclear if all of those functions required the third-party application that was selected to ensure the security of that data on their device, and when it was transmitted over the internet.

Recommendation: Review the use of work services on employees personal devices to ensure that all work-related activities are secured in an appropriate manner, and in accordance with NARO policies.

# Conclusions and Follow-on Activities

-Isai

The first paragraph should include a high-level summary of the assessment. Something like:

The assessment team found NARO applies industry best practices across all of their facilities, systems, and procedures. However, the team did identify several vulnerabilities that could be used by an attacker to compromise NARO systems and information. Of the vulnerabilities identified in Section 5, the team recommends the vulnerabilities related to backups be prioritized given the concerns related to ransomware attacks common to this business area.

For follow-on activities, the team recommends…

( heres what they did good. heres what they did bad. heres what they need to do mooving forward.)