ACME CORP

# Facility Security Assessment

June 3, 2025

This work was performed under contract to:

**Acme Corp**
Hollywood, CA,
United States

ioSENTRIX
Trusted by Security Conscious Companies

https://iosentrix.com
contact@iosentrix.com

CREST

# Revision History

| Version | Modification | Date | Author |
|---|---|---|---|
| 0.1 | Acme Corp – Facility Security Assessment | 2/21/2025 | ioSENTRIX |

# Document Confidentiality Statement

The information in this document is confidential to the person to whom it is addressed and should not be disclosed to any other person. It may not be reproduced in whole, or in part, nor may any of the information contained therein be disclosed without the prior consent of **ioSENTRIX LLC** ('the Company'). A recipient may not solicit, directly or indirectly (whether through an agent or otherwise) the participation of another institution or person without the prior approval of the directors of the Company.

Any form of reproduction, dissemination, copying, disclosure, modification, distribution and or publication of this material is strictly prohibited.

The information in this documentation is subject to change without notice and should not be construed as a commitment by the Company. The Company makes no representations or warranties, express or implied, with respect to the documentation and shall not be liable for any damages, including any indirect, incidental, consequential damages (such as loss of profit, loss of use of assets, loss of business opportunity, loss of data or claims for or on behalf of user's customers), that may be suffered by the use.

# Table of Contents

# Executive Summary

### Assessment Overview

Between February 16 and 17, 2025, ioSENTRIX conducted a Facility Security Assessment at Acme's Hollywood, CA headquarters building. The primary objective was to evaluate the security controls intended to keep unauthorized personnel out of the facility.

Testing consisted of two phases. First, ioSENTRIX performed evasive adversarial testing with the intent of gaining unauthorized access from the perspective of a disgruntled former employee, a capable consumer with grievances against the business, and/or an advanced Nation State threat. Upon competition of the evasive testing, ioSENTRIX transitioned to an exhaustive facility walkthrough. This enabled ioSENTRIX to identify various areas of improvement for Acme to harden their facility controls and policies.

### Evasive Facility Testing

ioSENTRIX started the assessment with remote reconnaissance. During this phase, ioSENTRIX was able to gather detailed information including the facilities floor plan, employee base, access control system, badge technology and layout. The bulk of this information was gathered from corporate and employee social media posts. This included video footage of an employee badging into the Acme office space and conducting a fairly detailed walkthrough of the facility.

Leveraging the information gathered from social media in conjunction with reviewing geospatial mapping data and publicly available leasing data, ioSENTRIX built a threat profile prior to arriving on-site. Once on-site, ioSENTRIX targeted Acme employees that wore corporate branded attire as they transitioned from the parking garage to the facility using commercially available longrange badge cloning equipment. ioSENTRIX was able to capture three employee badges within a short period before moving offsite. ioSENTRIX then wrote the captured badge data to blank access control cards that mimicked the aesthetic styling of Acme's HID ProxCard II cards this included designing a card reel that matched a Acme branded card reel that was identified on an employee's Instagram account.

During the evasive testing, ioSENTRIX had unrestricted access to Acme's offices on the second and third floors of the Corporate Centers at International Plaza building three (CCIII.). This included access to the network closets on the second and third floor. ioSENTRIX moved through the Acme office space on two separate occasions. During both time periods, no Acme employees engaged with ioSENTRIX. While inside the facility, ioSENTRIX noted that there were several file boxes near the legal department that were considered to be unsecure and potentially contain sensitive data. While walking through the facility, ioSENTRIX noted one (1) workstation that was left unattended in an unlocked state. Leveraging keystroke injection tools, it would take an attacker just a few moments to extract sensitive data or install malicious software.

In addition to gaining access to the facility using the compromised access control card data, ioSENTRIX removed the fabricated badges and tailgated Acme employees a total of five (5) times through various doors without confrontation.

### Facility Walkthrough

During the facility walkthrough, ioSENTRIX assumed a non-evasive role and looked each floors security controls as well as conducted a brief interview with Acme's facility manager. During this period note that one door on the third floor lacked sufficient latch protections as such, ioSENTRIX was able to loid the locking mechanism and bypass the RFID system. Similarly, ioSENTRIX was able to bypass the RFID systems on the network closets as the bottom door gap allowed the usage of an under-the-door tool (UDT) to actuate the handle from inside the network closet. Finally, while conducting the facility interview it was determined that the Acme and the facility lacked critical reactionary security control equipment, policies, and incident handling procedures.

### Remediation Strategy

#### *Access Control System*

ioSENTRIX recommends that Acme transition their internal access control cards to a solution that employs encrypted communication using proprietary keys (e.g., iCLASS SE / Seos with Elite Keys). Additionally, we recommend that Acme use access control cards that have a unique look that includes an employee photo, and a holographic marker. Doing so will reduce an attacker's ability to identify the specific technology in use and make creating a replica substantially more difficult. In addition, Acme should ensure that all doors have proper latch protections. This should include adding magnetic locking mechanisms to the inside of the network closets to prevent the usage of UDT devices. Finally, ioSENTRIX recommends adding security cameras to all protected doors and the networking closets. Doing so will help triage any incident as well as provide law enforcement agencies with tangible evidence when considering criminal prosecution.

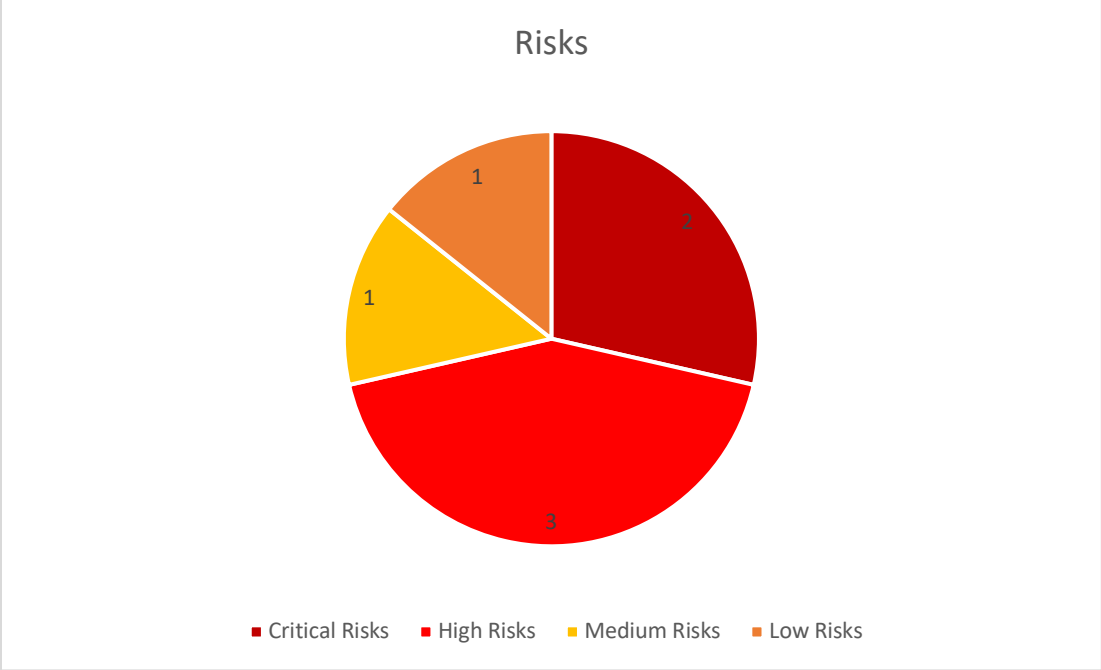
#### *Policy & Procedures*

# Dashboard

| | |
|---|---|
| **Name** | **Facility Security Assessment** |
| **Dates** | February 16, 2025, to February 17, 2025 |
| **Targets** | Acme Corp Headquarters Facility in Hollywood, CA |

## Findings Breakdown (Chart)

| | |
|---|---|
| **Critical Priority Risks** | **2** |
| **High Priority Risks** | **3** |
| **Medium Priority Risks** | **1** |
| **Low Priority Risks** | **1** |
| **Total Findings** | **7** |



# 1 Introduction

ioSENTRIX performed a Facility Security Assessment to assess vulnerabilities in security protocols, focusing on social manipulation and physical access control bypass methods, with the aim of bolstering Acme's defensive posture. This covert evaluation followed a Black Box methodology, knowing only the company name and in-scope physical structure addresses.

# 2 Methodology

ioSENTRIX performed the following strategic phases between February 16 and 17, 2025:

**Target Identification & Threat Profiling**

Collection of intel from various channels to craft optimal exploitation strategies. Review publicly accessible resources, including corporate web presence, geospatial data, social platforms, and physical surveillance to construct a holistic profile of business operations.

**Attack Execution**

Exploit intelligence harvested during the previous phase to circumvent physical access controls and/or manipulate personnel into executing predetermined actions, such as granting access to the in-scope physical structure.

**Findings & remediation**

Delineate the outcomes of each scenario and associated weak points identified throughout the engagement. Analyze each scenario to generate analytics and propose countermeasures, aiding the organization in mitigating exposed vulnerabilities.

## 2.1 Scope

Acme designated the following structure as in-scope for the purpose of conducting facility breach operations and the facility walkthrough:

| Site Name | Address |
|---|---|
| **Acme Headquarters Campus** | 123 Hello World St, Hollywood, CA 33607 (Suites 200 & 350) |

## 2.2 Information Gathering & Threat Profiling

Open-source intelligence (OSINT) aims to gather and examine openly accessible data about the target entity. ioSENTRIX developed a detailed overview of Acme's public digital footprint by leveraging various techniques. This process involved scrutinizing publicly available resources, including search engine results, externally accessible web platforms, social media profiles, and geospatial data.

### 2.2.1 Remote Reconnaissance: Social Media Analysis

During this process, ioSENTRIX gathered information from Instagram and Facebook and then manually reviewed it for any sensitive data or signs of security weaknesses. The screenshots below illustrate exam les of ex osed Acme data that was recovered.

Figure 1: RFID System Identification (Datawatch Systems (HID) multiCLASS SE RP10 Reader)

Figure 2: HID ProxCard II Badge Identification (Badge Layout #1: HID ProxCard II)

Figure 3: Badge Exposure Policy (Badge Layout #2: Datawatch Systems branded ProxCard II)

Figure 4: Employee Enumeration Badge & Lanyard Layout (Employee [redacted]o)

Figure 5: Employee Enumeration (Office Manager [redacted])


Figure 6: Employee Enumeration (Influence Operations)

ioSENTRIX recommends removing the following Instagram Reels as well as similar content that may disclosure sensitive information regarding the facility, security controls, and building layout. This includes content that ties faces and names to specific locations and/or functions within the facility. While this information may seem benign, in cases where a disgruntled employee or a consumer with a grievance may leverage the small details to identify where employees reside, travel, etc. in an effort to cause physical harm.

| URL | Description |
|---|---|
| [redacted] | Badge Exposure Policy, Employee Name/Job Function/Desk Location, E-mail Exposure, Detailed Facility Layout |
| [redacted] | Badge Exposure Policy |
| [redacted] | Badge Exposure Policy |
| [redacted]/ | Badge Exposure Policy. We recommend that the user remove photos within the "Work/fit" highlights that contain badge photos and other potentially sensitive corporate information. |

### 2.2.2 Remote Reconnaissance: Geospatial Observations & Facility Details

During this phase of reconnaissance, ioSENTRIX performed a detailed review of the Corporate Centers at International Plaza located on Boy Scout Blvd. in Hollywood, CA. The primary focus was to identify details regarding security operations, tenant information, general layout and access controls/deterrents.

Figure 7: Corporate Centers at [redacted] Layout

ioSENTRIX was able to determine that [redacted] consisted of [redacted] floors (292,357 sqft.) and while the site stated that "24x7 security was available". The campus lacked sufficient camera coverage and roaming guards to be able to accurately identify and triage a physical security incident.

Figure 8: [redacted] w/o Security Camera Coverage

ioSENTRIX utilized Google Street view and evaluated street level images around the building. This was used to help with identifying entry and exit points before confirming these with on-site surveillance. In total ioSENTRIX found four (4) entry points and to including one loading dock. The following screenshots illustrate points of ingress/egress as well as specific points of interest that were leveraged during the attack scenarios. While badging technology readers were visible in the Street View images, they lacked sufficient clarity to make a positive identification of the specific technology.

Figure 9: Visitor Entrance (EN1)

Figure 10: Employee Entrance (EN2 / Loading Dock)

Figure 11: Employee Entrance (EN3)

Figure 12: Community Trash Receptacles

Figure 13: [redacted] Employee Entrance [redacted]

The courtyard was selected for badge cloning because of its proximity to the building and the garage where employees would be parking.

Figure 14: Garage Entrance (Open Gate)

It was noted in the Google Street View that the garage entrances were left open during business hours.

### 2.2.3 On-site Reconnaissance: Facility Layout & Reference Graphic

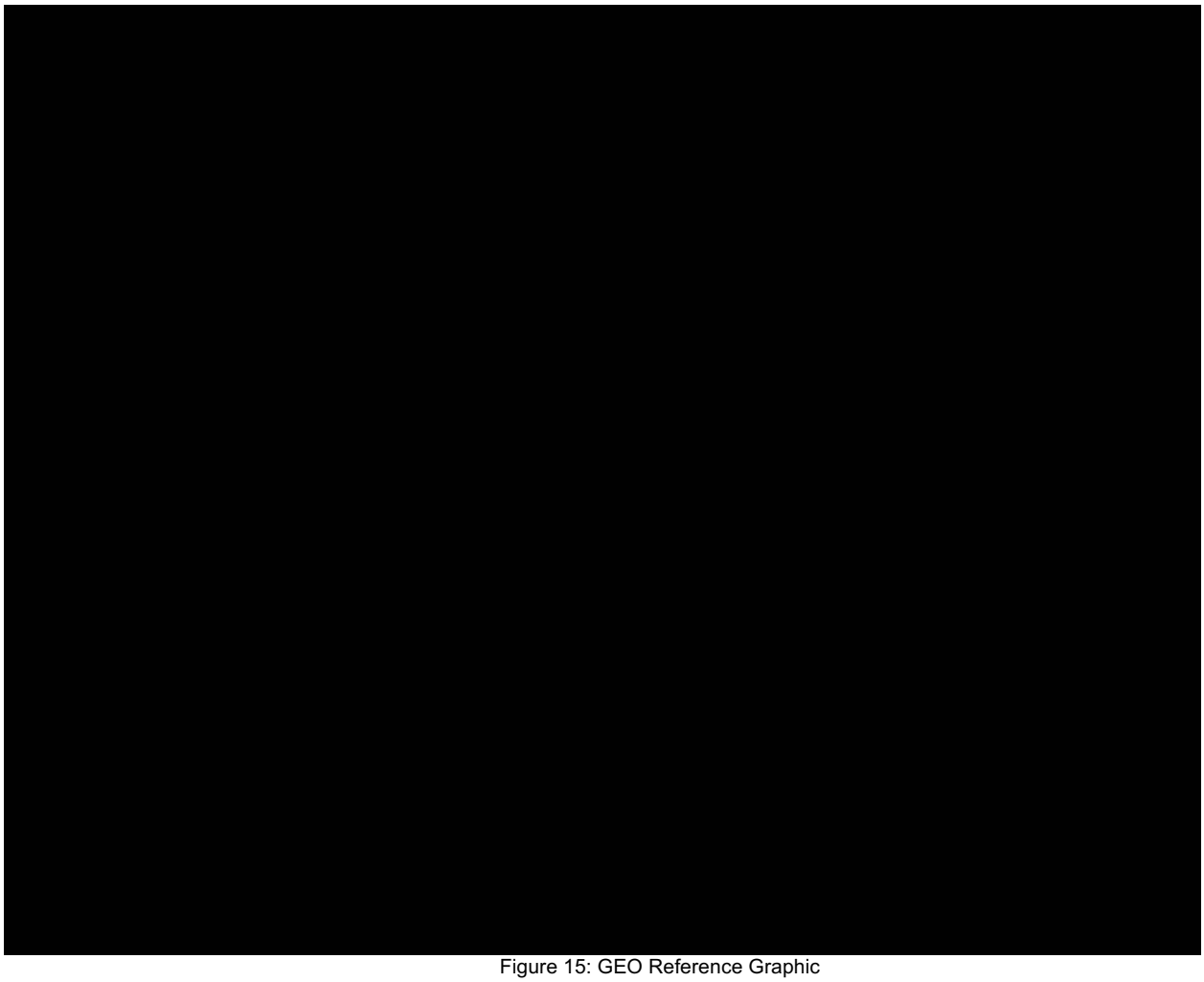


Figure 15: GEO Reference Graphic

Highlighted in red in the above graphic are the primary entry points, while onsite it was noted that EN3 did have an onsite security guard at a desk. Additionally, ioSENTRIX found EN2 to be the facility loading dock. G1, G2, and G3 garage entrances were open during business hours. Finally Point-of-Interest 1 (POI1) was used during badge cloning badge cloning operations.

## 2.3 Attack Execution

Following a comprehensive assessment of publicly available information, ioSENTRIX conducted an in-depth analysis to identify potential attack vectors and evaluate their likelihood of success. Based on this analysis, our team devised and implemented a series of attack scenarios. These scenarios employed a multi-layered approach, combining various techniques to circumvent both physical security measures.

The subsequent sections of this report provide a detailed breakdown of the attack path used, vulnerabilities discovered, and outcomes achieved during this process.

### 2.3.1 Attack Scenario #1

| Attack Method | Results |
|---|---|
| Badge Cloning | Successful |

On February 16, 2025, at approximately 08:33 AM, ioSENTRIX conducted on-site reconnaissance at the Corporate Centers at International Plaza campus. During this operation, ioSENTRIX leveraged longrange doppelgänger RFID cloning devices that were concealed inside of satchels that specifically targeted HID Prox access control cards. Doppelgänger weaponizes legitimate RFID readers to capture and interpret the card data. HID Prox Card II (H10301) is considered legacy and dangerous access control technology since it does not offer encryption making it trivial to capture cards using well known commercially available tooling.


Figure 16: Doppelgänger RFID Longrange Cloning Device

ioSENTRIX leverage the staircase within the parking garage to capture cards as Acme employees exited. This spot was specifically chosen as it offered a narrowing chokepoint and lacked security camera coverage. Additionally, ioSENTRIX was able to be highly targeted as a large number of Acme employees wore corporate branded clothing.

Figure 17: Parking Garage Badge Cloning Position

The following cards were compromised during the engagement this operation:

| Bit Length | Facility Code | Card Number | Notes |
|---|---|---|---|
| 26 | XXX | XXXX | Standard Employee Badge |
| 26 | XXX | XXXXX | Standard Employee Badge |
| 34 | XXX | XXX | Network Administrator |

With the captured card data, ioSENTRIX was able to use a Proxmark3 device with Doppelgänger Assistant to write the card data to blank T5577 cards. In doing this, the T5577 cards directly emulated the captured values and card type. Making them indistinguishable from the legitimate employee badges when presented to the facilities access control system.

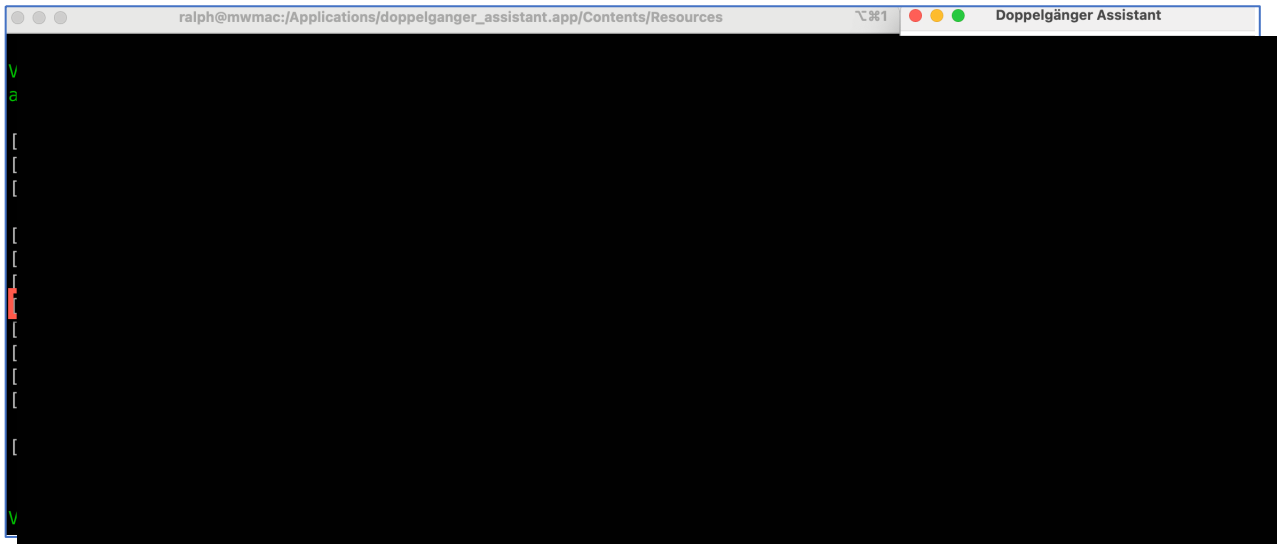



Figure 18: Writing the Captured Access Control Card Data

In addition to writing the access control card data to the T5577 cards, ioSENTRIX attempted to match the badge branding and layout that was referenced above in the Remote Reconnaissance section.

Figure 19: Fabricated Badges

### Internal Facility Reconnaissance / Badge Validation

On Monday February 16, 2025, ioSENTRIX made two separate entries into the facility. The first entry was at 11:30 am to confirm that the captured badges worked to access floors two and three via the elevator and staircase. It was noted that while badge access was required to depress the level two button, card access was not required to access the third floor. This may be by design, given that Acme is not the only occupant on third floor.

Figure 20: Badge Access Required for Floor #2 Only

Figure 21: No Badge Required for Floor #3

Figure 22: Badge Required for Entry on Floor #2

Upon confirming access, ioSENTRIX departed the facility at approximately 11:45 AM.

### Building Evening Entry

At approximately 5:31 PM, ioSENTRIX returned to the facility and entered suites 350 and 200. While inside the facility, ioSENTRIX noted that several employees were still working. However, at no point was ioSENTRIX confronted while inside the building.

Figure 23: Facility Access

While moving through the facility, ioSENTRIX inspected work areas for unattended sensitive documents and unlocked workstations. While there were no unlocked workstations, ioSENTRIX identified unsecured files within the Legal area.

Figure 24: Insecured Sensitive Documents

ioSENTRIX exited the facility at approximately 5:45 PM after moving through suites 200 and 350. The morning of February 17, 2025, ioSENTRIX returned to the facility to perform a facility walkthrough. While conducting the walkthrough, ioSENTRIX made an additional pass through both office spaces and attempted to access the networking closets with one of the captured access control cards. The captured card provided access to the closets located in the second-floor hallway and inside of suite 350.

Figure 25: Networking Closet Access

Additionally, while walking through the office space, ioSENTRIX noted one (1) unlocked and unattended workstation.

Figure 26: Unlocked Workstation

Finally, ioSENTRIX inspected a network printer and was able to browse the directory and historical metadata from the print logs. While is information does not present a direct threat by itself, it illustrates the username structure and username which can be leveraged to perform password guessing attacks.

Figure 27: Network Printer Inspection

### 2.3.2 Attack Scenario #2

| Attack Method | Results |
|---|---|
| Tailgating | Successful |

On February 17, 2025, between 11:30 and 11:45 AM, ioSENTRIX removed the fabricated badges and performed five (5) tailgating attempts into the second and third-floor office spaces. During these attempts, ioSENTRIX was not confronted indicating that tailgating is culturally accepted by the employee base.

Figure 28: Tailgating

Figure 29: Tailgating

Figure 30: Tailgating

These tailgating attempts concluded evasive testing.

## 2.4 Facility Walkthrough

As part of the facility walkthrough, ioSENTRIX performed the following actions:

- Conducted a detailed review of each external door
- Inspected trash receptacles and shred bins for sensitive information and unsecured locks
- Performed an interview with the Office Manager

The following represents noteworthy observations based on the facility walkthrough.

| Security Control | Result / Observation |
|---|---|
| **Security Cameras & Monitoring** | • The CCIII common areas lacked sufficient camera coverage to triage and/or prosecute physical security instances. These controls were limited to the parking garage vehicle entrances.<br>• Acme office space lacked sufficient camera coverage to triage and/or prosecute physical security instances. At a minimum, ioSENTRIX recommends that cameras be installed at all ingress/egress points as well as inside sensitive areas such as networking closets. |
| **Security Guard Presence** | • The CCIII facility maintained a singular security guard that appeared to be stationary during operations. It is recommended a facility of that size maintain both stationary and roaming guards. |
| **Facility Access Windows** | • Acme limited the majority of employees access to work hours only (6AM – 9PM). If possible, more granular controls should be assigned to shift work employees allowing access for one hour before and after the intended work shift. |
| **Mechanical Latches** | • The majority of mechanical latches maintained proper latch guard protections. However, one latch on the third floor was missing the latch guard which enabled ioSENTRIX to manipulate the latch and bypass the RFID system. |
| **Vertical & Horizontal Air Gaps** | • The double doors on Suite 200 and Suite 350 maintained adequate gap protections which made sensor and latch tampering difficult/not possible.<br>• The networking closest maintained a large enough gap for ioSENTRIX to pass an Under-the-Door Tool (UDT) into the closet and manipulate the latch from inside. It's recommended that Acme install a 3,000lb or greater magnetic lock and Push-to-Exit button on the inside of the networking to prevent access control system bypass. |
| **RFID Access Control System** | • The Datawatch Systems RFID readers support multiCLASS SE technology which offers the ability to use |

| | |
|---|---|
| | cryptographically secure cards with proprietary keying material. However, Acme uses unencrypted HID Prox cards which are easily cloneable. ioSENTRIX recommends that Acme use the current cards only to access the facility and gym and transition all office spaces to iCLASS SE/Seos with Elite keys.<br>• Employee badges leveraged generic branding that defined the card technology that was in place at the Acme facility. This makes badge replication trivial. We recommend that Acme use unique cards that contain the employees name, photo, and a holographic maker. Company name and logo can be omitted. |
| **Badge Exposure Policy** | • Employee routinely wore their badges off their hips outside of Acme office space. This makes them easy targets for badge cloning operations. We recommend employing a policy that requires badges be worn above the waist while inside the facility and requires employees to remove their badges prior to exiting the facility.<br>• Several instances of badging information were collected from Acme and employee social media accounts. The Badge Exposure Policy should explicitly require that employees do not take photos while wearing their badges. |
| **Active Shooter Policy & Incident Response Planning** | • It is critical that Acme develop and train for both active shooter and incident response. Over the past five years active shooter incidents have increased 89% over the previous five years. In 2024, there was 586 mass shooting events, resulting in 711 deaths and 2,375 injuries. We recommend reviewing the following FBI resource page.<br>○ https://www.fbi.gov/how-we-can-help-you/active-shooter-safety-resources |

Figure 31: Missing Deadlatch Strike Plate (Suite 350)

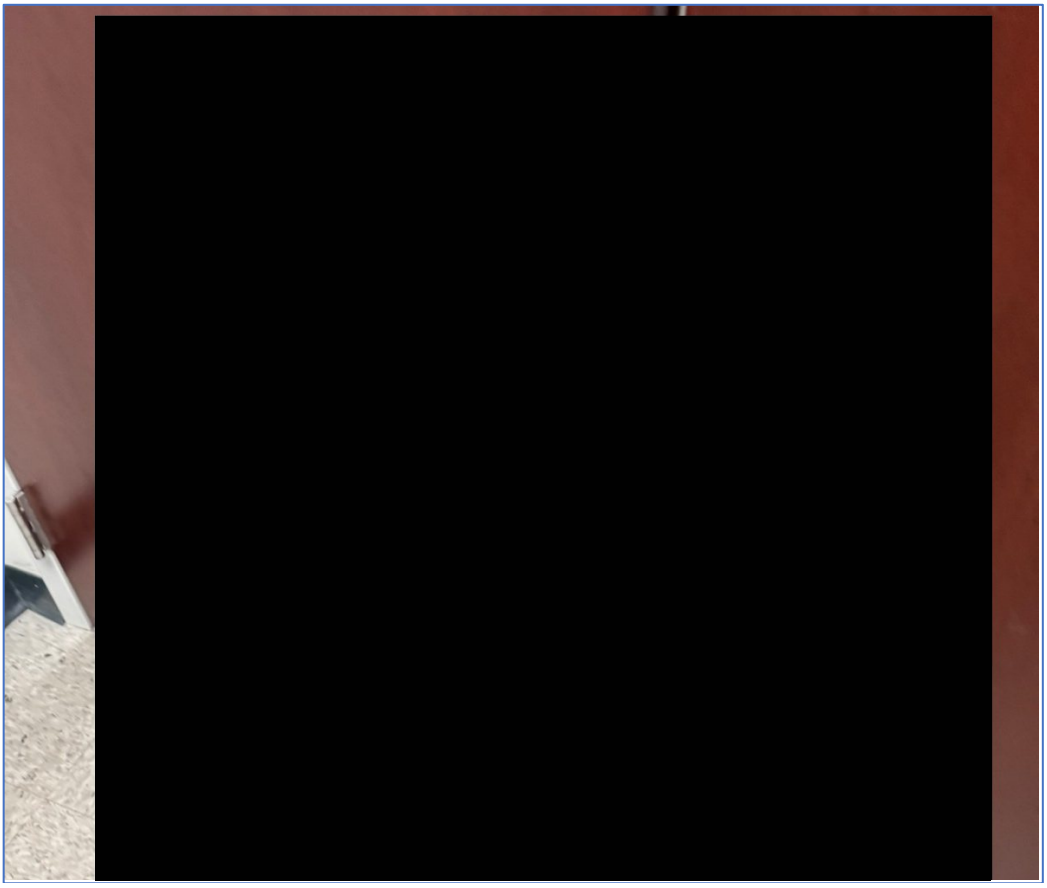


Figure 32: Under-the-Door-Tool (UDT) Network Closet

# 3 Findings & Remediation Guidance

### 3.1.1 Severity rankings

ioSENTRIX ranks the severity of a risk using a method developed by the United States National Institute of Standards and Technology (NIST). Calculating risk severity as a derived value, based upon mitigation and impact assessments. The risk value represents the technical risk to the software and is calculated using the table below.

| | | Impact | | | | |
|---|---|---|---|---|---|---|
| Likelihood | | **Critical** | **High** | **Medium** | **Low** | **Informational** |
| | **Critical** | Critical | High | Medium | Low | Informational |
| | **High** | Critical | High | Medium | Low | Informational |
| | **Medium** | High | Medium | Medium | Low | Informational |
| | **Low** | Medium | Low | Low | Low | Informational |
| | **Informational** | Low | Low | Informational | Informational | Informational |

Table 1: NIST Risk Severity Matrix

In the above table, the Likelihood is defined as the probability of a given threat exploiting the vulnerability. That incorporates ease of exploitation and determination and capability of the given threat agent. The impact is defined as a possible impact of occurrence of a risk.

The levels of risk severity have the following meanings:

- **Critical:** A critical risk is characterized by a very high likelihood and a high or very high impact. Remediation must be prioritized immediately and scheduled as the highest priority. Critical issues are considered blockers for new releases and must be resolved before deployment.
- **High:** High-severity issues present a substantial risk, though they may not block new releases. Remediation should be scheduled promptly and treated as a high priority.
- **Medium:** Medium severity issues require remediation. The organization should create and implement a remediation plan to address these risks effectively.
- **Low:** For low-severity issues, the organization may choose to either mitigate the risk or formally accept it, depending on its risk tolerance and strategic priorities.
- **Informational:** Informational findings have minimal or no direct impact on the target scope. However, they are reported as they may contribute to risk under specific circumstances, such as when combined with other vulnerabilities or technologies. Remediation is optional.

### 3.1.2 Assessment Limitations

The ever-changing technology landscape and the increasing sophistication of attacks are reasons for which no entity can truthfully claim to identify all the security issues, nor guarantee the lifetime-security of an organization. Note that this point-in-time assessment was based on the best-effort and was performed only on the environment provided by Acme. Thus, changes to the environment may impact the applicability of the results provided herein.

ioSENTRIX cannot guarantee 100% coverage for any security assessment.

# 4 Technical Risks

## 4.1 Summary of findings

Below is the summary of the vulnerabilities found during the assessment. Complete details are available in the later section of this report.

| No | Security Risk | Severity | Status |
|---|---|---|---|
| **5.1.1** | Unencrypted / Easily Cloneable Access Control Card Technology | Critical | Open |
| **5.1.2** | Employee Base is Susceptible to Tailgating / Piggybacking | Critical | Open |
| **5.2.1** | Oversized Door Gaps Allowed Tampering / Manipulation | High | Open |
| **5.2.1** | External Doors Lacked Proper Latch Protections | High | Open |
| **5.2.1** | Ineffective Badge Exposure Policy | High | Open |
| **5.3.1** | Information Disclosure: Network Printers | Low | Open |

# 5 Findings

## 5.1 Critical Severity Risks

### 5.1.1 Unencrypted / Easily Cloneable Access Control Card Technology

| Risk Rating | Impact | Likelihood |
|---|---|---|
| Critical | Critical | High |

**Description:**

Acme's office space leverages deprecated and unencrypted access control card technology that is easily cloneable with commercially available tooling.

An attacker can leverage longrange cloners to capture employee badges at a distance without detection. The captured data can then be written to a blank card. When presented to the reader, the fake card is indistinguishable by the access control system, allowing unauthorized access.

**Impacted Assets:**

- Acme Headquarters

**Evidence:**

Reference Attack Scenario #1 for detailed information regarding this vulnerability.

**Remediation:**

ioSENTRIX recommends that Acme use the current cards only to access the facility and gym. Transition all office spaces to a card technology that uses proprietary cryptographic keying materials such as iCLASS SE/Seos with Elite keys. In addition, ioSENTRIX recommends that Acme use unique cards that contain the employees name, photo, and a holographic maker. Company name and logo can be omitted. Doing so will increase the skill and level of effort required to make a replica badge.

### 5.1.2 Employee Base is Susceptible to Tailgating / Piggybacking

| Risk Rating | Impact | Likelihood |
|---|---|---|
| Critical | Critical | High |

**Description:**

Individuals exhibited vulnerability to tailgating / piggybacking.

Tailgating poses a significant security risk by allowing unauthorized individuals to gain access to restricted areas without proper authentication, potentially leading to theft, data breaches, or physical harm.

**Impacted Assets:**

- Acme Employees

**Evidence:**

During Attack Scenario #2, ioSENTRIX was able follow employees into suite 200 and suite 350 a total of five (5) times without confrontation.

**Remediation:**

ioSENTRIX recommends offering training on the dangers of allowing others to following employees through badge protected doors. In addition, signs should be placed at each entrance as a reminder that the Acme office space is considered a secure area and as such, each employee is required to badge in.

## 5.2 High Severity Risks

### 5.2.1 Oversized Door Gaps Allowed Tampering / Manipulation

| Risk Rating | Impact | Likelihood |
|---|---|---|
| High | Critical | Medium |

**Description:**

The facilities doors were either misaligned, improperly installed or missing adequate seal protection resulting in an air gap large enough to pass physical security bypassing tooling into the facility.

Improper door gaps can allow a malicious attacker to manipulate locking mechanisms and gain unauthorized entry.

**Impacted Assets:**

- Acme's Network Closets

**Evidence:**

ioSENTRIX was able to send an under-the-door tool (UDT) underneath the network closet doors to acuate the inside handle and bypass the RFID reader as illustrated above.

**Remediation:**

Alter the door clearances to reduce or completely remove the air gap. This change will stop external manipulation of the internal handle. Additionally, the networking closets should have a 3,000lb or great magnetic lock installed at the top of the door to prevent bypass attempts.

### 5.2.2 External Doors Lacked Proper Latch Protections

| Risk Rating | Impact | Likelihood |
|---|---|---|
| High | Critical | Medium |

**Description:**

A door in the hallway of suite 350 was missing the deadlatch strike plate.

Without proper latching protections, an attacker can use a loiding tool to manipulate the latch and bypass the RFID system.

**Impacted Assets:**

- Hallway Door into Suite 350

**Evidence:**

For more information, reference the screenshot above.

**Remediation:**

Add a deadlatch strike plate to the affected door frame and ensure that the deadlatch is properly engaged.

### 5.2.3 Ineffective Badge Exposure Policy

| Risk Rating | Impact | Likelihood |
|---|---|---|
| High | High | Medium |

**Description:**

The organization's access control policy either does not require employees to conceal their badges while outside the corporate facility, does not prohibit posting badge photos on social media, or the policy is not being enforced.

An attacker can readily examine the badge design and layout, making it possible to create replica employee badges from discreet locations like parking structures, third-party venues, or even social media.

**Impacted Assets:**

- Acme Headquarters
- Acme Employees
- Acme Social Media

**Evidence:**

During preliminary investigation, ioSENTRIX noted that most employees displayed their Acme identification badges openly while outside the CCIII facility. Furthermore, ioSENTRIX discovered multiple cases where Acme and an employee shared images of the corporate badging system and access control cards to social media.

The following Instagram posts were identified:

- [redacted]

**Remediation:**

The following recommendations apply:

- **Concealment Outside Premises:** Personnel should be required to ensure that access badges remain out of sight when not within company facilities.
- **Visible Display Within Facilities:** While inside all corporate facilities, all employees must prominently display their access cards above waist level
- **Photographic Exclusion:** Access cards and associated control systems should be strictly prohibited from appearing in any photographic imagery, regardless of the official or unofficial nature of such documentation.

## 5.3 Medium Severity Risks

### 5.3.1 Insufficient Security Camera Coverage

| Risk Rating | Impact | Likelihood |
|---|---|---|
| Medium | High | Medium |

**Description:**

The Corporate Centers at International Plaza and the Acme office space lacked adequate security camera coverage.

The absence of security cameras in a corporate facility increases the risk of unauthorized access, theft, and workplace violence going undetected, making it harder to investigate incidents. Without surveillance, there is no visual deterrent against criminal activity, and employees or visitors may feel less secure. Additionally, the lack of recorded footage can hinder liability protection, compliance with security policies, and the ability to respond effectively to security breaches.

**Impacted Assets:**

- Acme Headquarters
- Corporate Centers at International Plaza

**Evidence:**

The only cameras observed during testing were positioned to capture employees entering through the vehicle gates in the parking garage.

**Remediation:**

Deploy security cameras at key entry points, high-risk areas (server rooms, cash handling areas), and parking lots, ensuring footage is recorded and retained.

## 5.4 Low Severity Risks

### 5.4.1 Information Disclosure: Network Printers

| Risk Rating | Impact | Likelihood |
|---|---|---|
| Low | Low | Low |

**Description:**

Network printers allowed access to the historical print metadata and the address book. While this information does not present a direct threat by itself, it exposes the username structure and email address which can be leveraged to perform password guessing attacks.

**Impacted Assets:**

- Acme Network Printers

**Evidence:**

Reference Attack Scenario #1 for detailed information regarding this issue.

**Remediation:**

If possible, set network printers to require a password prior to viewing print logs or the address book.

# About ioSENTRIX

ioSENTRIX LLC is a Security Consulting firm now proudly accredited by CREST, an internationally recognized hallmark for professional cybersecurity services. As a CREST accredited pentesting company, we adhere to the highest standards of service, ensuring that our clients receive the most comprehensive and reliable security testing available.

We provide a wide range of security consulting services to clients worldwide. Our clientele includes Fortune 500 companies, large enterprises, small start-ups, financial institutions, and several high-tech companies. At ioSENTRIX, we are committed to delivering innovative cybersecurity solutions.

As an innovative consulting company, we offer a full range of cyber security services tailored to businesses of all sizes and budget requirements. Our focus is on helping clients identify, mitigate, and prevent vulnerabilities in their software, infrastructure, and cloud environments.

Our comprehensive vulnerability assessment includes design-review, threat modeling, penetration testing, code review, and open source software security. We are equipped with the necessary tools and expertise to secure your business, allowing you to focus on growth and innovation.

Learn more about how our CREST accreditation and our services can benefit your business at **https://www.iosentrix.com.**

**ioSENTRIX LLC.**

13800 Coppermine Rd, Suite 190
Herndon Virginia 20171 (USA)

**Sales:** 1 (888) 958-0554
**Email:** sales@iosentrix.com