Criminal Justice Information Services (CJIS)

Security Policy

Introduction

- **Who am I?**

  Roy Kestler - Network Security Specialist - McLean County

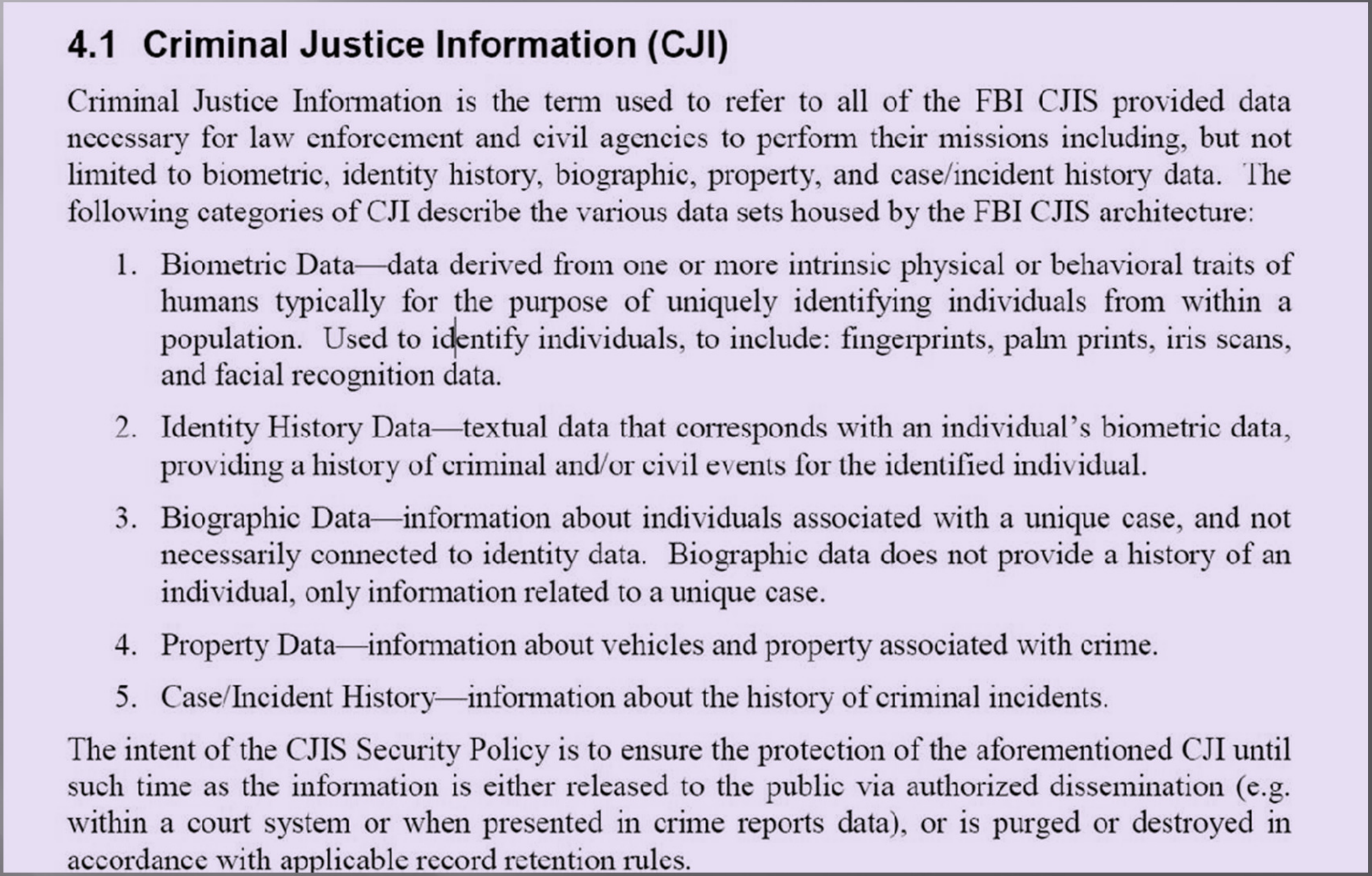
- **Purpose of this session**
- To provide you with pointers to the various sections of the CJIS Security Policy Version 5.1 which you may find useful while working towards or maintaining CJIS compliance.

- **Is this information available online?**

  Yes, the full CJIS Security Policy is available online at:

http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center

What is CJIS? – Section 4.1



4.1 Criminal Justice Information (CJI)

Criminal Justice Information is the term used to refer to all of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data. The following categories of CJI describe the various data sets housed by the FBI CJIS architecture:

1. Biometric Data—data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. Used to identify individuals, to include: fingerprints, palm prints, iris scans, and facial recognition data.
2. Identity History Data—textual data that corresponds with an individual's biometric data, providing a history of criminal and/or civil events for the identified individual.
3. Biographic Data—information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.
4. Property Data—information about vehicles and property associated with crime.
5. Case/Incident History—information about the history of criminal incidents.

The intent of the CJIS Security Policy is to ensure the protection of the aforementioned CJI until such time as the information is either released to the public via authorized dissemination (e.g. within a court system or when presented in crime reports data), or is purged or destroyed in accordance with applicable record retention rules.

Auditing and Accountability – Section 5.4

What should be logged?

When do we need to conduct audit reviews?

What is the record retention period?

AUDIT CHECKLIST

☑ Audit Satisfactory

□ Non-conformances found

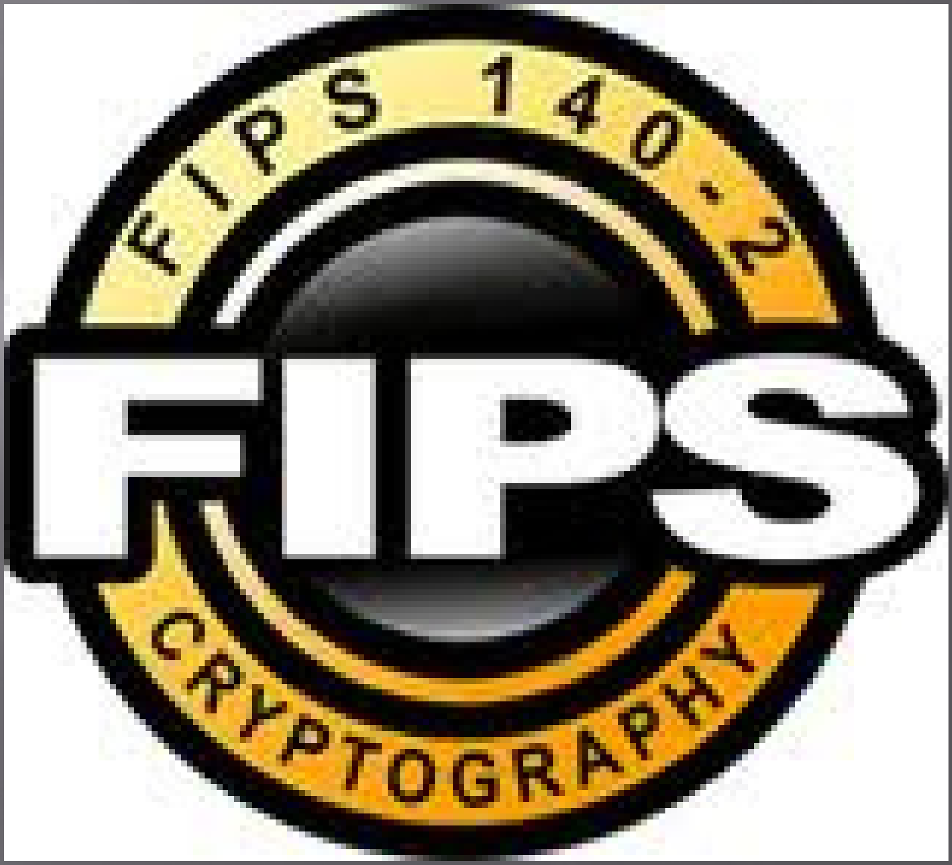
□ Observations made

Access Control – Section 5.5

Ensure access enforcement mechanisms utilize FIPS 140-2 cryptography

Information system controls shall restrict access to privileged functions

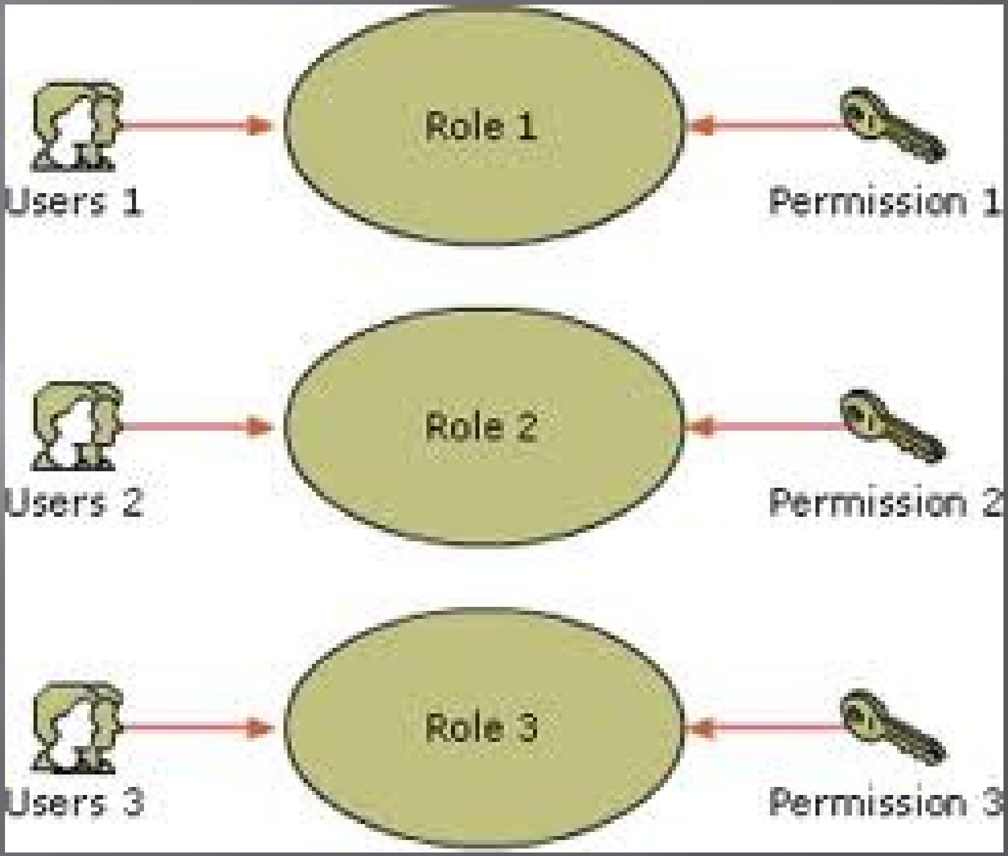
Enforce the most restrictive rights needed by users to perform their tasks



Role Based Access Controls assign users to roles and permissions

Access Control Lists control access between users and objects in the system

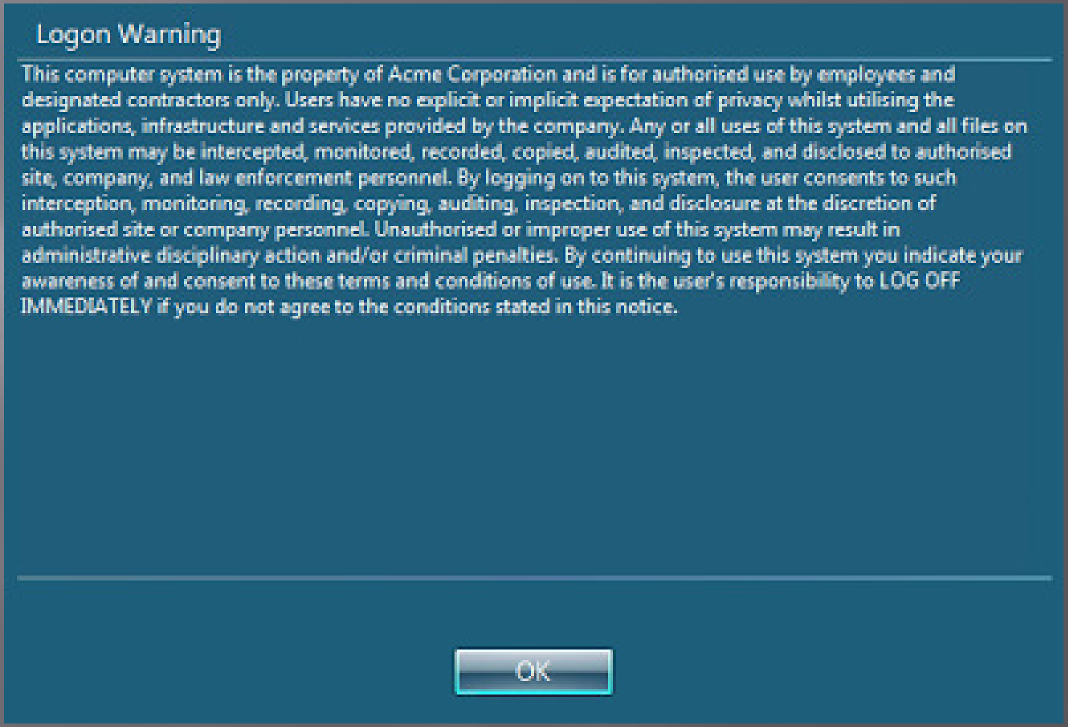
Users should be granted access on a “Need to know basis”



Display an approved system use notification.

Limit unsuccessful logins to a max of 5 and minimum lockout of 10 min.

Initiate a session lock after a maximum of 30 minutes of inactivity



Logon Warning

This computer system is the property of Acme Corporation and is for authorised use by employees and designated contractors only. Users have no explicit or implicit expectation of privacy whilst utilising the applications, infrastructure and services provided by the company. Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, inspected, and disclosed to authorised site, company, and law enforcement personnel. By logging on to this system, the user consents to such interception, monitoring, recording, copying, auditing, inspection, and disclosure at the discretion of authorised site or company personnel. Unauthorised or improper use of this system may result in administrative disciplinary action and/or criminal penalties. By continuing to use this system you indicate your awareness of and consent to these terms and conditions of use. It is the user's responsibility to LOG OFF IMMEDIATELY if you do not agree to the conditions stated in this notice.

802.11x Wireless Protocols

- Ensure rogue AP’s do not exist
- Maintain a complete inventory of all AP’s
- Place AP’s in secured areas
- Change the default SSID in the AP’s
- Disable the broadcast SSID feature
- SSID name can’t contain agency ID information
- Encryption keys must be at least 128 bit
- Disable nonessential protocols
- Enable logging and review logs monthly

Identification and Authentication - Section 5.6

Where can Standard Authentication be used?

Password requirements:

Minimum of 8 characters

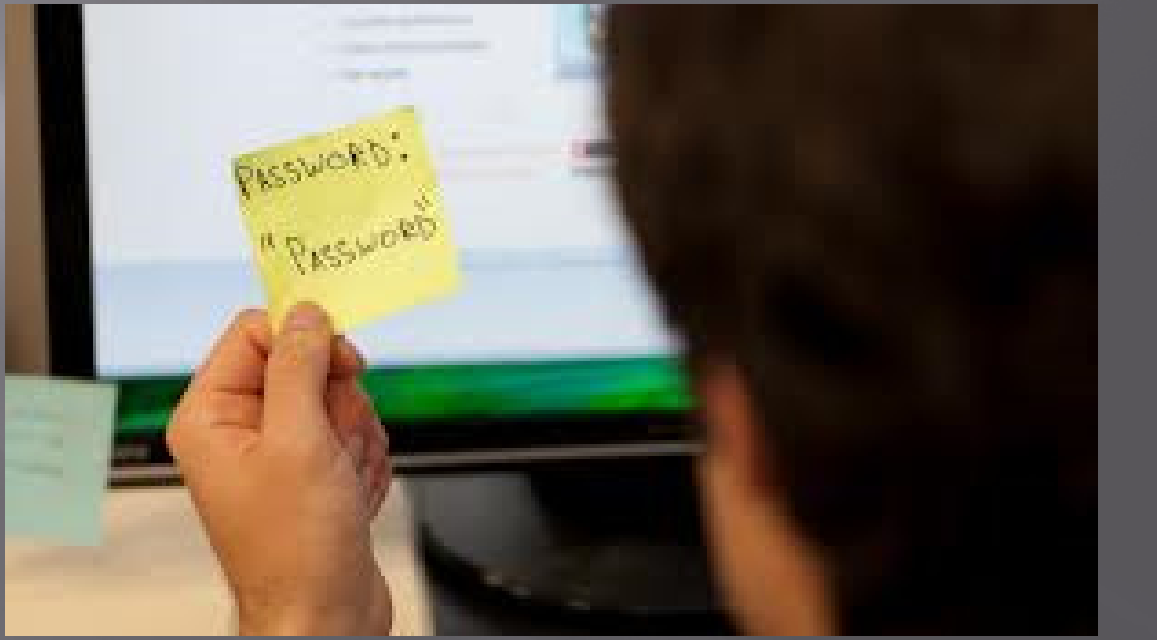
No words

Different than user ID

Expires within 90 days

Unique to 10 historically

Cannot be displayed



Strong passwords don’t have to be hard to remember!

Example Sentence:

Show me an example of a Strong password!

Break down:

1. Take the 1st letter of each word in your sentence.
2. Make the word you want to emphasize a capital letter.
3. Throw in a number you can change easily to obtain a unique password but keep it in the middle.
4. End it with the punctuation from your sentence.

Your new strong password is: **smaeoaSp1!**

Advanced Authentication - Policy and Rationale

Each user must be uniquely identified

Two-Factor Authentication is required for locations not physically secured

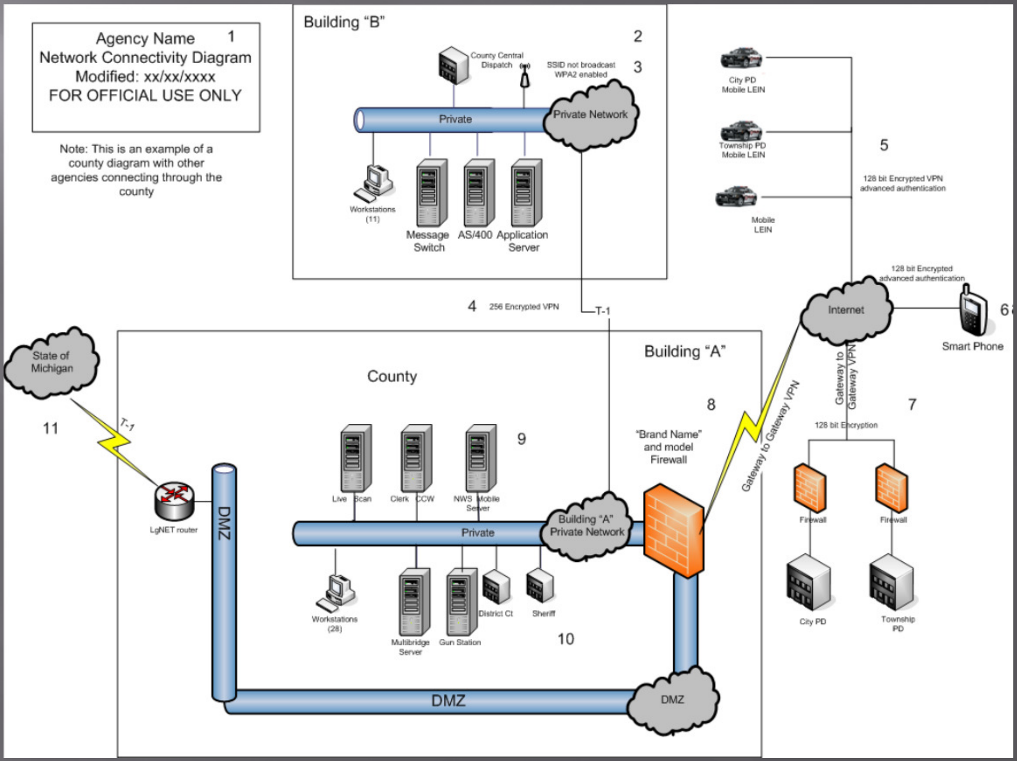
In a physically secure area visitor logs and escorts are required

Configuration Management – Section 5.7

Configure the systems to provide only essential capabilities

Provide a topographical drawing of both physical & logical connections

Mark drawing For Offical Use Only with agency name & modification date



Media Protection - Section 5.8

Securely store electronic and physical media within physically secure area

Maintain written documentation of steps taken to destroy media

Physical Protection – Section 5.9

The Agency shall control all physical access points to secure locations

A police vehicle is considered a physically secure location until 30Sep13

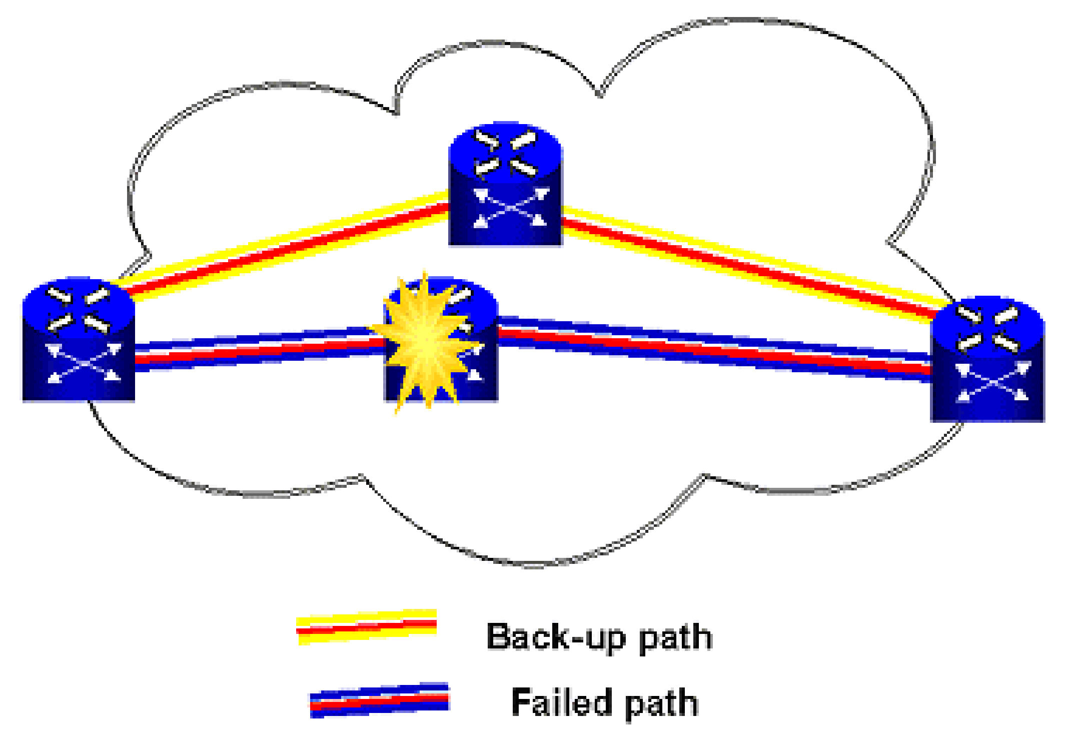
Visitor access records will be maintained for a minimum of 1 year

System & Communications Protection & Information Integrity Section 5.10

Boundary Protection equipment should fail closed in event of a failure

Employ personal firewalls on all mobile devices (laptops,PDA's, etc.)

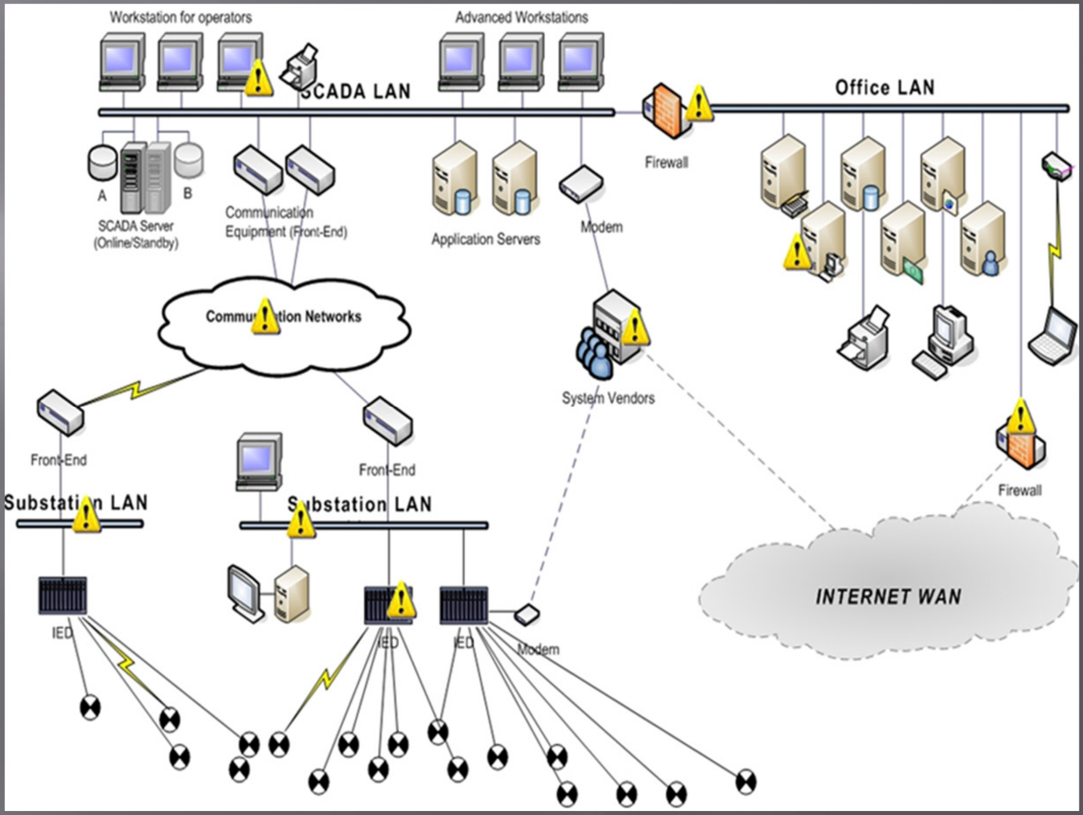
Send logs to a central logging facility for correlation and analysis



Employ virus & spyware protection on all networked computing devices

Implement policy that ensures prompt installation of security patches

Deploy spam protection mechanisms at critical system entry points



Encryption

When transmitting or storing CJIS data outside of physically secure locations, encrypt it.

The current minimum is to be at least 128 bit encryption

CJI transmitted via facsimile is exempt from encryption requirements

Why are these policies important to me?

Stuxnet was a targeted attack against an Iran uranium purification plant.

Security procedures were in place at the plant so how did it fall victim?

The same process could be utilized to attack CJIS information.

Conclusion

Today we touched on key points of the

CJIS Security Policy version 5.1
(CJISD-ITS-DOC-08140-5.1)

Note: Version 5.2 is now available

http://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center