



**Process Control Systems  
Industry Conference**

# **A Trusted Framework for Managing Compliance Evidence**

**Jeff Kalibjian**

**HP Atalla Security Products**

**[jeff.kalibjian@hp.com](mailto:jeff.kalibjian@hp.com)**

Copyright© 2008 HP Development Corporation

# The Overwhelming Challenge of Compliance Data Management!!!



# NERC CIP 002-009 Cyber Security Standards are comprehensive & demanding

NERC CIP	Description
CIP-002-1	Critical Cyber Assets
CIP-003-1	Security Management Controls
CIP-004-1	Personnel and Training
CIP-005-1	Electronic Security
CIP-006-1	Physical Security
CIP-007-1	Systems Security Management
CIP-008-1	Incident Reporting Response Planning
CIP-009-1	Recovery Plans

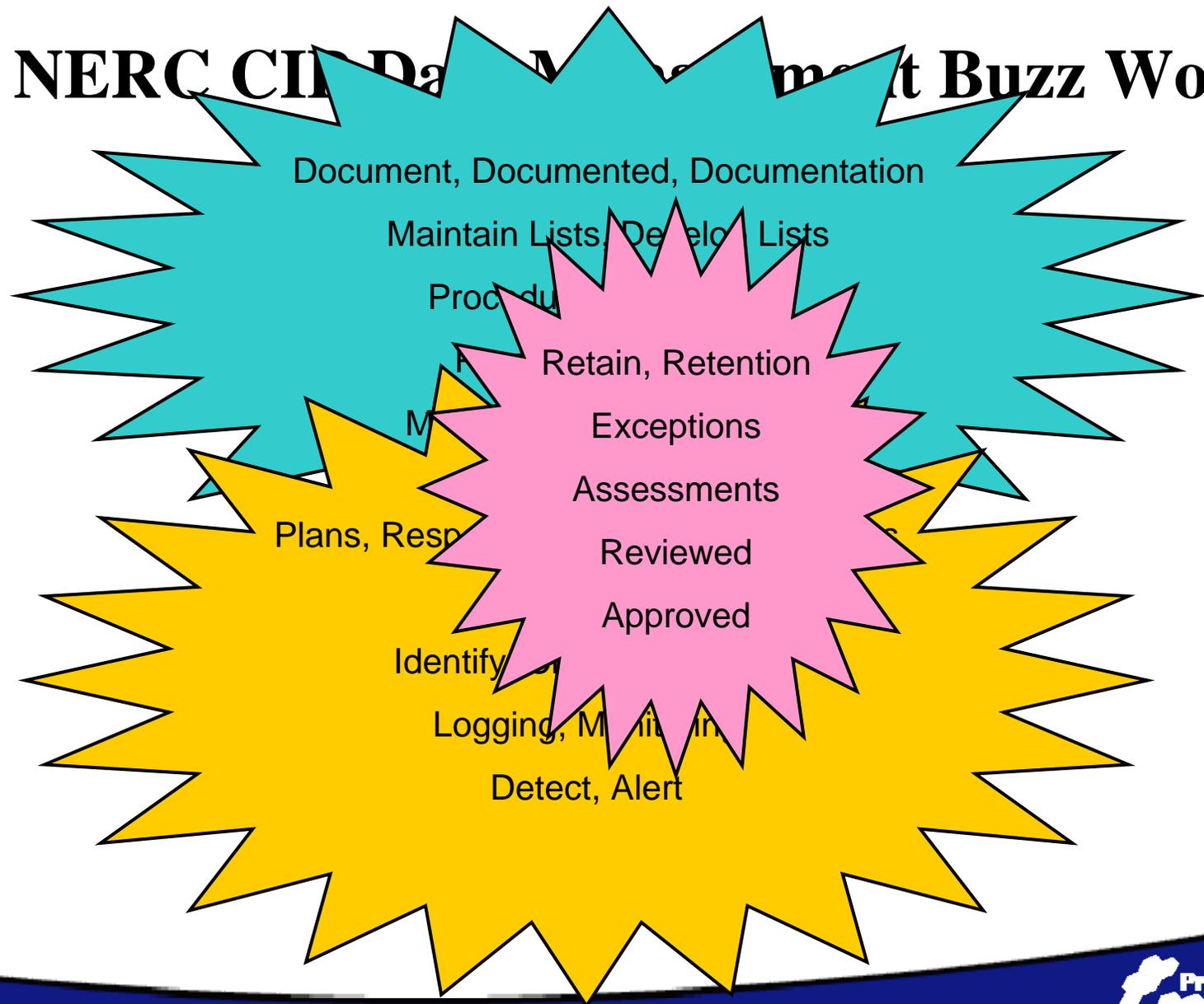
- ◆ **Must create or save sensitive operations data**
- ◆ **Requires documents, drawings, logs and other types of files**
- ◆ **Periodic review and management approval**
- ◆ **Annual audits**

# Five Important Aspects of NERC CIP 002-009 Cyber Security Standards

## ◆ Requirements and measures

- Implying deployed technology
  - Firewalls, intrusion detection, video surveillance, etc.
- Implying developing procedures/policies
  - Disaster recovery, security, policy, etc.
- Implying defining and enforcing configurations
  - Access controls, usable ports, etc.
- Collecting, managing, reviewing, approving, auditing compliance evidence
  - Event logs, training plans, processes, procedures, etc.
- Serving Data
  - Security plans, training, etc

# NERC CIP Data Management Buzz Words



# Totals

## ◆ CIP-002

- 1 documentation, 2 lists, 1 approval

## ◆ CIP-003

- 3 documentation; 1 approval

## ◆ CIP-004

- 5 documentation, 1 list, 1 review

## ◆ CIP-005

- 11 documentation, 2 review, 3 process, 2 logs, 2 asses, 1 detect, 1 alert, 1 monitor

## Totals (cont.)

### ◆ CIP-006

- 4 documentation, 2 review, 3 process, 2 logs, 3 plan, 2 procedure, 1 monitor, 1 retain, 1 records, 1 retention

### ◆ CIP-007

- 8 documentation, 4 process, 1 review, 2 logs, 5 procedure, 1 alert, 2 monitor, 2 methods, 1 audit, 2 asses

### ◆ CIP-008

- 1 documentation, 1 plan

### ◆ CIP-009

- ! review; 1 plan

# Event Log Collection

- ◆ **NERC CIP-005-1**

- R3, R3.1, R3.2, R5.3, M3, M5;

- ◆ **CIP-006-1**

- R4.1, R5 R6.3, M4, M5;

- ◆ **CIP-007-1**

- R5.1.2, R6, R6.1, R6.2, R6.3, R6.4, R6.5, M6

# Your Compliance Data is....

- ◆ Information an auditor reviews to assess your adherence to standards
- ◆ A detailed description of your control system network
- ◆ A unique view into your business processes
- ◆ Evidence that could clear your enterprise of responsibility should something go wrong
- ◆ Data that can help better define configuration setting information of critical devices



# “Static” Compliance Process

- ◆ Acquire Data
  - Human generated
  - Computer generated
- ◆ Review
- ◆ Certify
- ◆ Audit

# “Dynamic” Compliance Process

- ◆ Acquire Data
  - Human generated
  - Computer generated
- ◆ Review
- ◆ Certify
- ◆ *Update/Enforce*
- ◆ Audit

# Compliance End Game: *Audit and....*

## ◆ High Stakes

- Stay in business
- Stay in business with sanctions
- Go out of business

## ◆ High Value

- Dollar value of penalties
- Dollar value of lost revenues

# Enforcement

- ◆ Insure policy is reflected in settings/configurations of critical cyber assets
  - Not good enough to have intent
    - Must demonstrate implementation

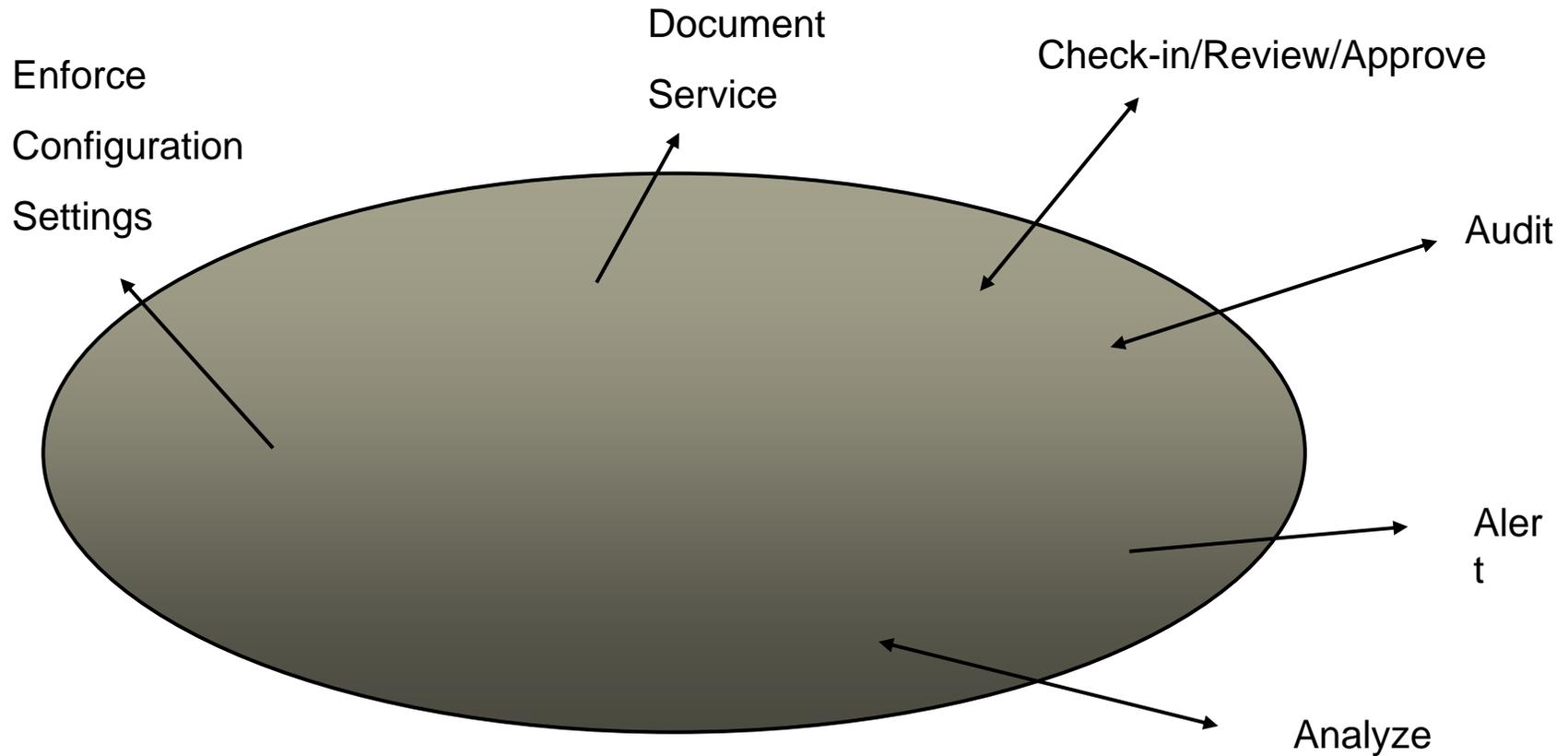
# Compliance Costs

- ◆ Human driven
  - Time consuming
  - Costly
  - Error prone
- ◆ Computer driven
  - Efficient
  - Cost effective
  - Comprehensive

# Compliance Goal

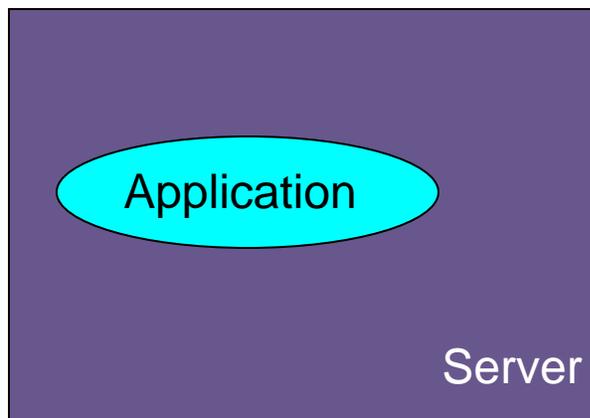
- ◆ Leverage computer technology!
  - Automate as much as possible
    - Log collection
    - Analysis and reporting
    - Configuration/settings update
- ◆ Leverage technology breakthroughs from other compliance verticals

# The Compliance Automation Process



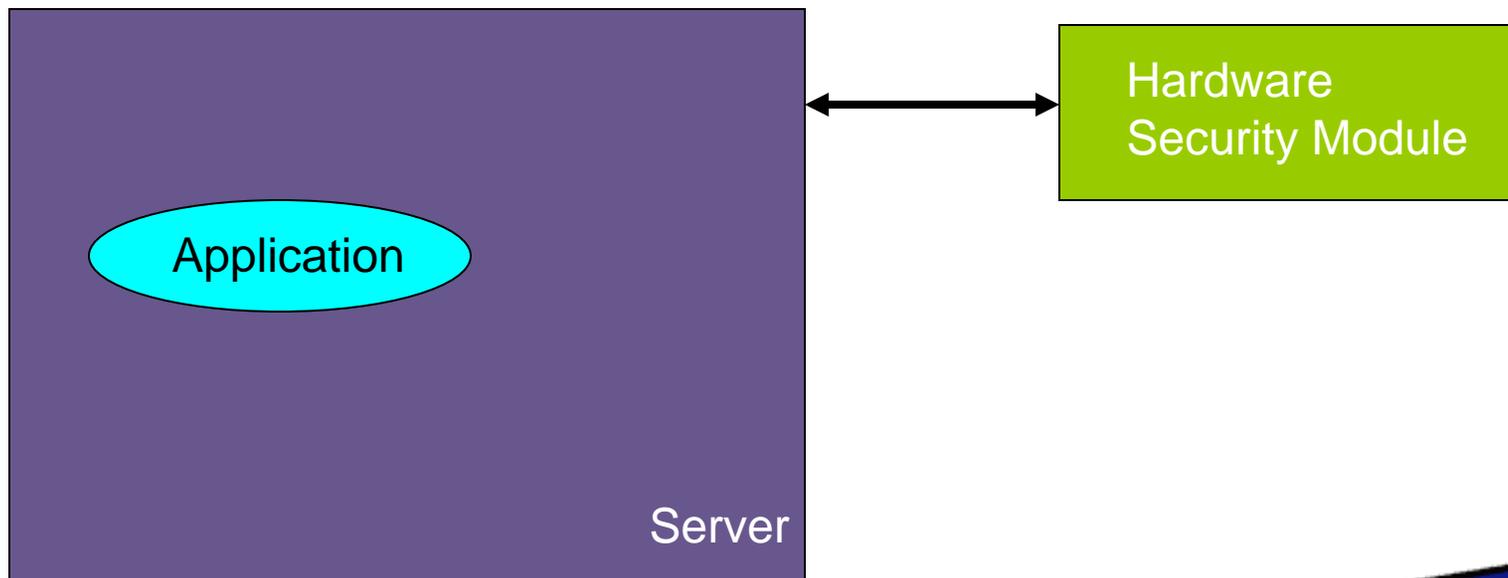
# Security differentiator

Most applications requiring security are architected as a monolithic application that runs on a generic client or server and utilizes software based security libraries



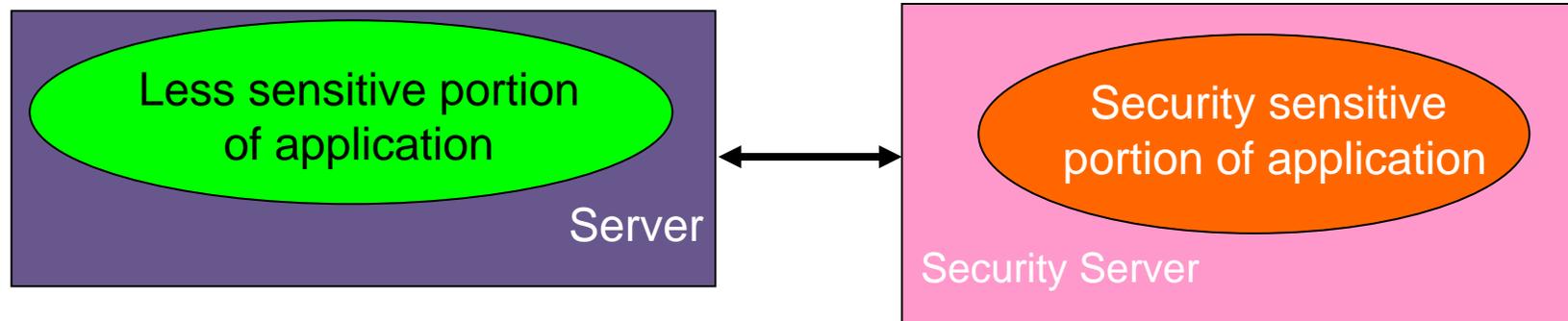
# Security differentiator

More sophisticated applications requiring security use a FIPS 140-2 certified hardware security module that provide cryptographic functionality and protects keys



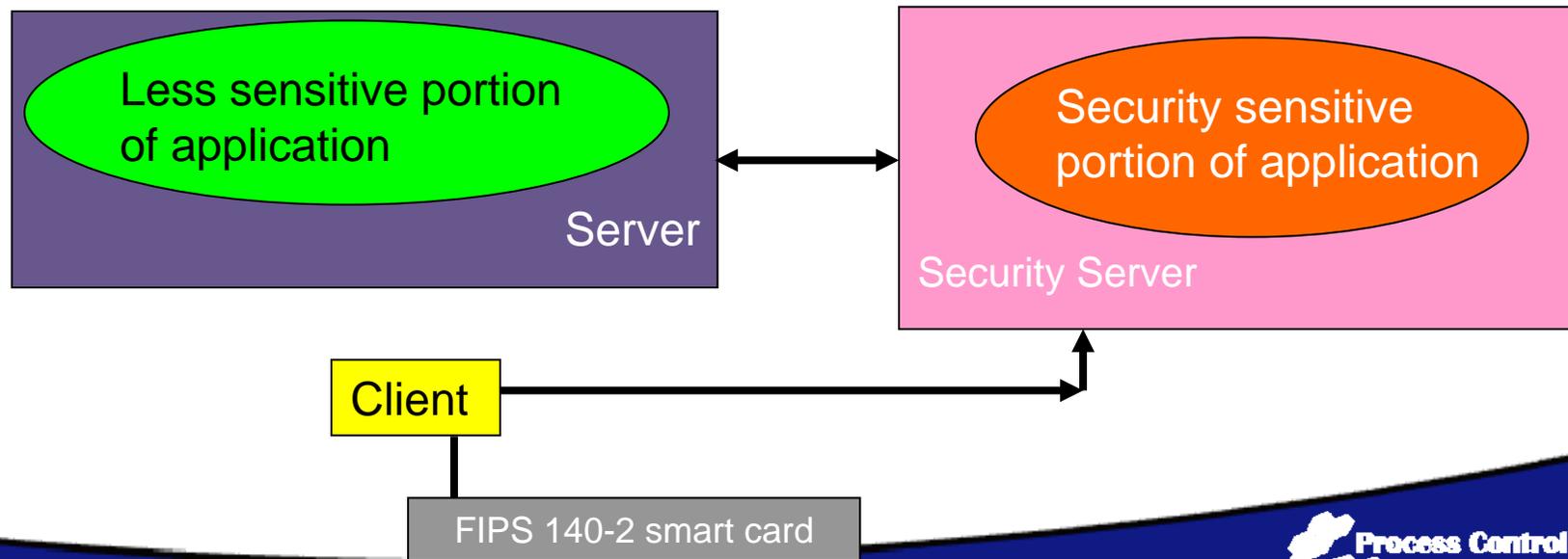
# Security differentiator

In the HP paradigm the actual security sensitive portions of the application are run on a FIPS 140-2 Level 4 certified Security Processor that can not only perform cryptographic operations and protect keys, but run application code protected by a Common Criteria certified operation system



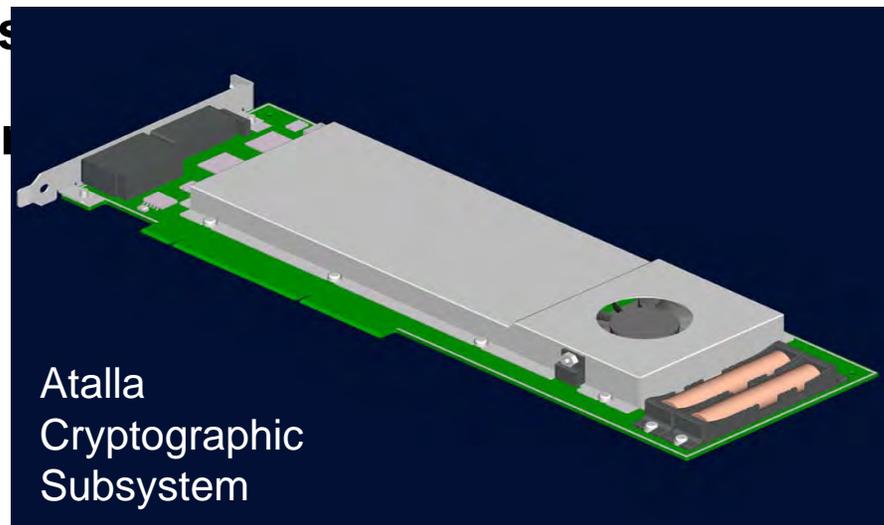
# Security differentiator

Further, any interaction with users is secured with a FIPS 140-2 Level 3 Smart Card----facilitating creation of a secure tunnel between the user at the client and the sensitive software running in the Atalla Cryptographic Subsystem



# FIPS 140-2 Level 4 certified hardware is the 'heart' of the compliance solution

- ◆ All security, policy, critical logic, and configuration decisions take place in an anti-tamper hardware module (Level 4 is highest)
- ◆ Runs a Common Criteria EAL 6+ operating system
- ◆ Stops attacks on cryptographic processing, critical system



# NIST specifies FIPS 140-2 levels for hardware-based security modules

Federal Information Processing Standard (FIPS) that specifies four levels of increasing security requirements within a system protecting sensitive information

Level 4	All of the protections in Level 3 plus protections against environmental condition changes such as temperature and voltage changes
Level 3	Requires strong enclosures or tamper detection and response circuitry that can zero-ize sensitive data. Level 3 also requires identity based authentication mechanisms
Level 2	Requires tamper evidence by utilizing tamper evident coatings or seals, role based authentication
Level 1	No specific physical security mechanisms required

# ISO: Common Criteria (Software)

Common Criteria is an ISO standard (15408) and has seven increasing Evaluation Assurance Levels (EAL)

<b>EAL - 7</b>	Formally verified design and tested. Advanced security engineering and development techniques that can be rigorously mathematically modeled and analyzed.
<b>EAL - 6</b>	Semi-formally verified design and tested. Security engineering techniques applied to an advanced development environment.
<b>EAL - 5</b>	Semi-formally designed and tested. Rigorous commercial development tools and specialty security design techniques to design and implement TOE
<b>EAL - 4</b>	Methodically designed, tested, and reviewed. Used when developers ??
<b>EAL - 3</b>	Methodically tested and checked. Evaluation of TOE is done at design stage.
<b>EAL - 2</b>	Structurally tested. Evaluation of TOE is done with respect to developer design information and test results.
<b>EAL - 1</b>	Functionally tested. Evaluation of Target of Evaluation (TOE) is done with respect to the customer documentation.

# Establishing Trust: Create a Security Services Framework

- ◆ Trusted time
  - Time source emanating from a FIPS 140-2 Level 3 or Level 4 boundary
- ◆ Digital signature
  - 2048 bit key
- ◆ Data encryption
  - AES 256 bit
- ◆ Key management
  - Data encryption key rotation
  - Identity re-issue
- ◆ Two factor authentication
  - Use FIPS 140-2 certified smart cards

## That is Used in a....

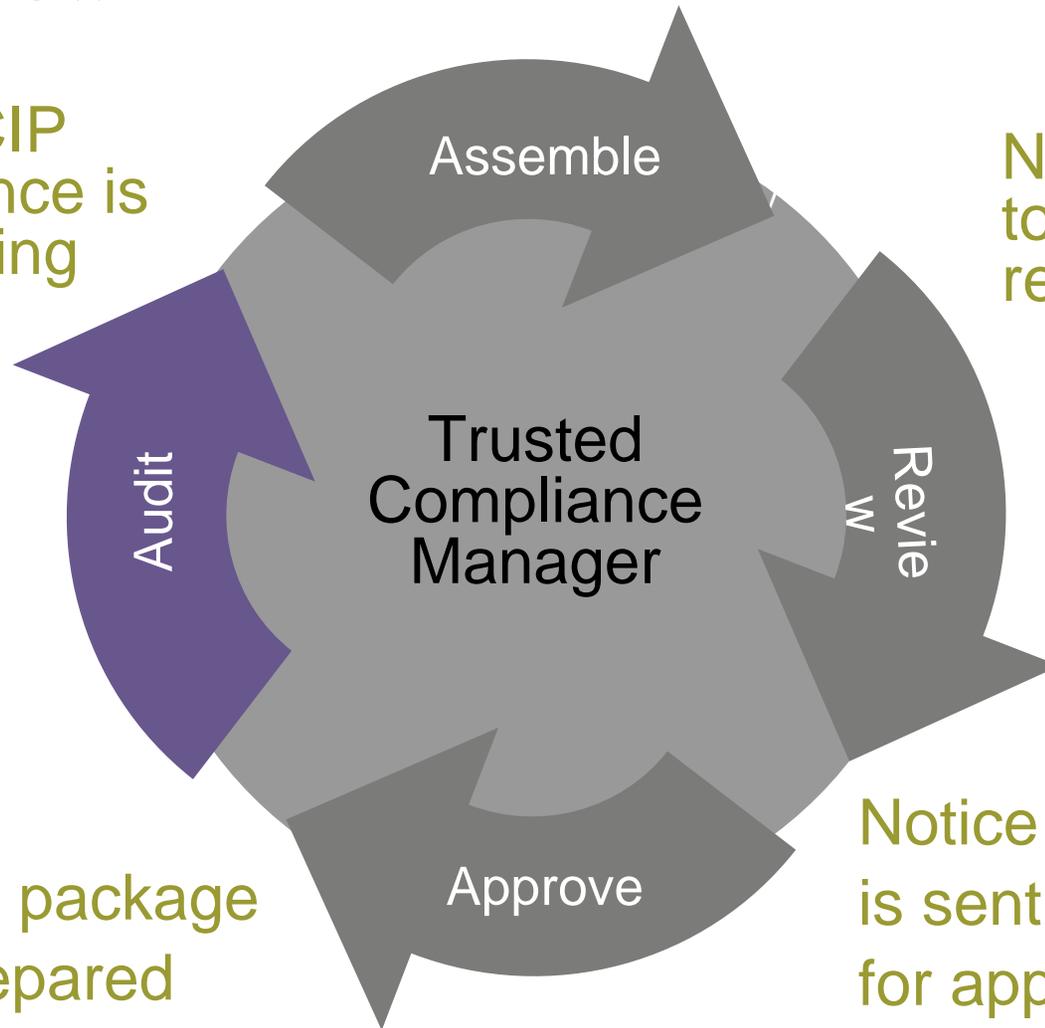
- ◆ Trusted infrastructure to automate and manage an organization's compliance evidence
  - Collect data (human generated and computer generated)
  - Check-in data
  - Review and/or modify (human generated) data
  - Approve data
  - Enforce/update configuration
  - Audit data
  - Serve data

## How?

- ◆ Leverage FIPS 140-2 and Common Criteria security technologies
  - Neutral third parties evaluate security implementation to standard

# NERC CIP Compliance Data Management Workflow

NERC CIP compliance is an ongoing process



Notice is sent to SME for review

Notice is sent to executive for approval

Audit package is prepared

# Check-in: What You Do

- ◆ Establish compliance evidence
  - Company created documents
  - Collected log/analysis/report data
  - Digitized data
- ◆ Specify applicable standard and measure
- ◆ Specify data type
  - Substantiation
  - Exception
  - Out of band
- ◆ Specify information security level
- ◆ Specify comments

# Check-in: What System Does

- ◆ Track document version
- ◆ Enforce encryption policy based on information security level selected
  - Check consistency with user information security level access privileges
- ◆ Place digital signature over data
- ◆ Place digital signature over check-in event
  - Person
  - Date/time
  - Comments
- ◆ Monitor next expected document actions
  - Expect review event

## Review: What You Do

- ◆ Review check in comments
- ◆ Review current version of document/data
- ◆ Make review comments
- ◆ Review action
  - Accept
  - Reject
- ◆ Check for measure data complete

# Review: What System Does

- ◆ Enforce workflow
- ◆ Place digital signature over review event
  - Person
  - Date/time
  - Comments
- ◆ Monitor next expected document actions
  - Expect approval event
- ◆ Note measure complete

## Revise: What You Do

- ◆ Check out data
- ◆ Revise with appropriate tool
- ◆ Check-in
- ◆ Provide check-in comment

## Revise: What System Does

- ◆ Enforce workflow
- ◆ Increment document version
- ◆ Save old version
- ◆ Place digital signature over revise event
  - Person
  - Date/time
  - Comments

## Approve: What You Do

- ◆ Read check-in/reviewer comments
- ◆ Review current version of document/data
- ◆ Make approve comments
- ◆ Approve action
  - Accept
  - Reject

# Approve: What System Does

- ◆ Enforce workflow
- ◆ Place digital signature over approve event
  - Person
  - Date/time
  - Comments
- ◆ Monitor next expected document actions
  - i.e. re-review alert

# Audit: What You Do

- ◆ Give credentialed auditor access to current versions of checked in data
  - Optional: access to
    - Check-in comment
    - Review comments
    - Approve comments
- ◆ Provide capability for auditors to make comments on checked-in documents/data
- ◆ Provide capability for auditors to indicate audit decision and make overall comments

# Audit: What System Does

- Enforces access privileges
- Shows auditor
  - Incomplete measures
    - Data not checked-in
    - Data not reviewed
    - Data not approved
- Keeps track of every action auditor takes
- Create snapshot of all current versions of checked in data
- Place digital signature over audit event
  - Person
  - Date/time
  - Measure comments
  - Overall Comments
  - Current versions of documents
  - Audit actions
  - Audit result

# Event Log Collection Basics

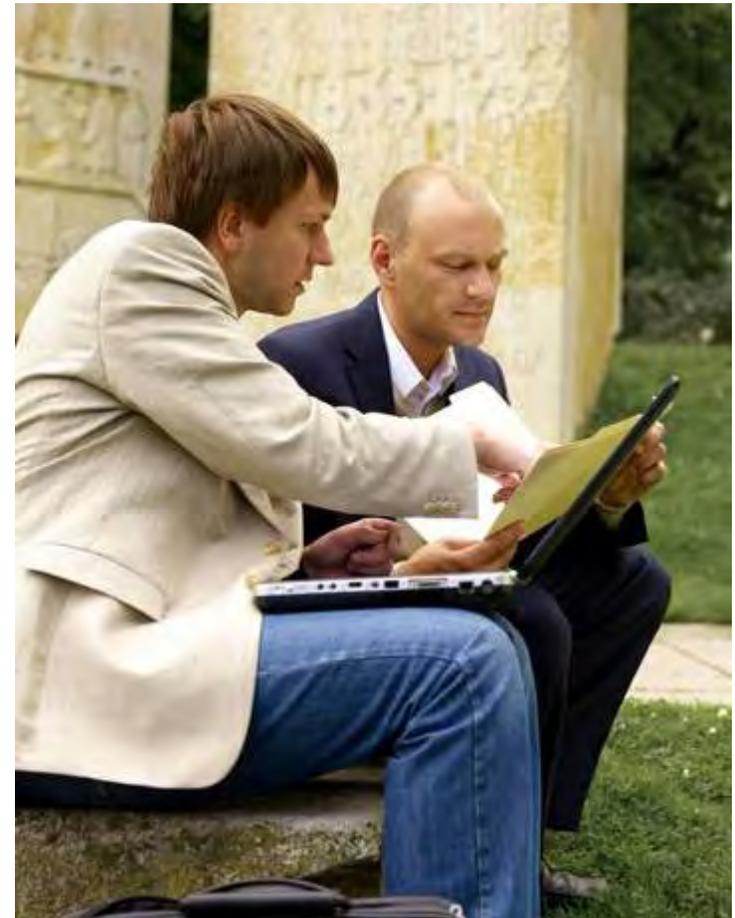
- ◆ **Talk to any device**
  - Understand any event log format
- ◆ **Collect as much data as possible**
- ◆ **Store as much data as possible**
- ◆ **Analyze collected event data in tractable period of time**
- ◆ **Produce meaningful results**
  - Confirm security posture
  - Confirm compliance
  - Identify threats



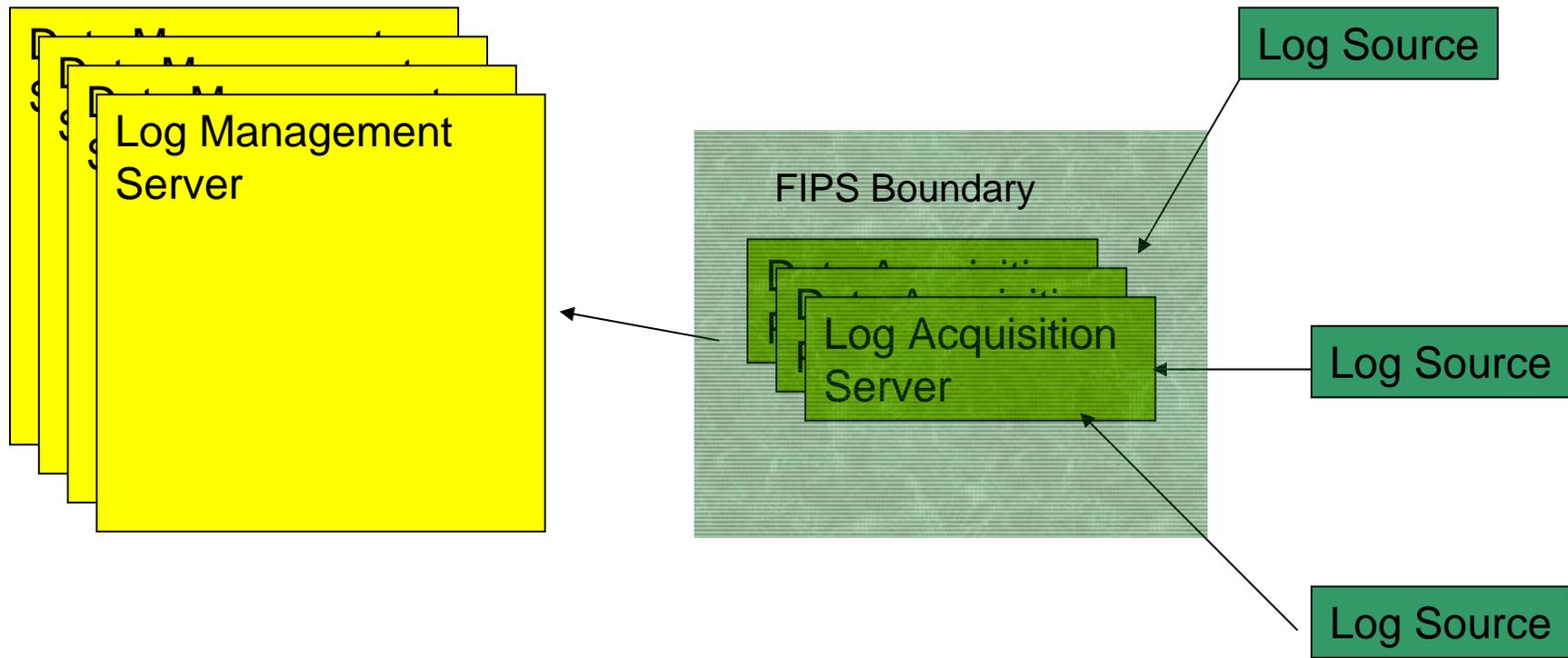
# It sounds so simple

## ◆ But...

- Most event log collection products require changes to event log data format
- .Have very limited storage capability
- Can take tens of hours for analysis
- Are difficult to deploy and maintain



# Event Log Collection Framework



# Conclusion

- ◆ Compliance data management
  - Don't try it manually
- ◆ Your compliance data has great value
- ◆ Leverage security technology to create trusted framework
  - FIPS 140-2
  - Common Criteria
- ◆ Utilize four step process
  - Check-in
  - Review/modify
  - Approve
  - Audit

# Contact Information

## ◆ Jeff Kalibjian

- Phone: 925-785-3737
- E-mail: [jeff.kalibjian@hp.com](mailto:jeff.kalibjian@hp.com)