MOBILE DEVICE DISCUSSION:

MOSTLY RISK BASED SECURITY, BUT SOME OTHER STUFF THAT PACO WANTED ME TO TALK ABOUT
There are two policy models that are widely used today; rule-based and risk-based.

Traditionally, rule-based policies were developed to control computing assets at a time when regulatory compliance and security risk didn't even merit a passing thought.

The premise of rule-based approaches was simple enough in that the rules outlined what could or could not be done in a given environment or system. As time passed, complexities in distributed systems, such as pervasive computing environments and the internet, chipped away at the effectiveness of rule-based policies.
The majority of Law Enforcement organizations are still using a check box mentality as part of a compliance-driven approach to security. This method achieves point-in-time compliance certification rather than improving the Agency's true security posture.

In an attempt to give Law Enforcement managers the ability to identify and manage security risks, a new approach to security policies is needed.

This approach to policy doesn't focus on static rules but rather degrees of risk at any given time.
Security Risk is:

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of

1) the likelihood of occurrence; and
2) the adverse impacts that would arise if the circumstance or event occurs

Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.
Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization.
Residual Risk:

It is not possible to identify all risks, nor is it possible to eliminate all risk. The remaining risk is called "residual risk".

For any given risk, management can choose to accept the risk based upon the relative low value of the asset, the relative low frequency of occurrence, and the relative low impact on the business.

Or, leadership may choose to mitigate the risk by selecting and implementing appropriate control measures to reduce the risk.

The reality of some risks may be disputed. In such cases leadership may choose to deny the risk.

What do we see when we look at the CJIS Security Policy?
Chief Taylor, Amarillo PD, submitted a request to the APB to not require visitor logs for his office. It interfered with “Community Policing” and provided no value.

S+A, with FBI urging, voted to make no substantive changes – defining a “visitor” to a Secure Location.

APB rejected the motion and sent it back to S+A.

FBI (ISO and Legal) recommended no change, S+A changed it to be applicable to computer rooms and network closets.

APB rejected the motion and struck the requirement from the policy.

The visitor log, required by the CSP, had NEVER been used for any purpose.

Status – Awaiting the FBI Director’s signature.
CSP Version 5.0 set the date for the exemption of police vehicles to expire at the end of September, 2013. Police vehicles will not be considered a secure location and must use Advanced Authentication (AA).

The CSA for the State of New York submitted a request to delay:
- Too large an expense
- The date was not selected for a specific reason
- There has never been a security issue with vehicles

**Status** – will be reviewed at the Spring 2013 S+A Committee meeting.
Current Activity:
Non-Blackberry cellular devices (Part 1)

Current policy only allows Blackberry devices by requirements, not name.

RIM is consistently loosing market share and is under financial pressure. Their devices have not been well received in the consumer marketplace.

Government agencies, long the Blackberry stronghold, are evaluating and switching to non-Blackberry devices. More financial pressure.

Law Enforcement Agencies and Vendors have been asking for the ability to connect Apple and Android devices to the Law Enforcement network. Some vendors have had Apps available for a year or more.
Law Enforcement across the country have been using iPads, iPhones, various Android devices for their non-CJIS work.

94% of Fortune 500 companies use iPads for their business.

ICE Press Release:
Apple’s strict control of the hardware platform and operating system, independent of the telecommunication service provider, provides ICE, the principal investigative arm of the Department of Homeland Security, with the greatest degree of control and management to ensure reliable services to its mission users, according to the document for justification of the award. More than 17,600 users in U.S. Immigration & Customs Enforcement (ICE) are being moved from their BlackBerry devices to Apple's iPhone. (10/23/12 – IDG News Service)
Apple has sold over 100 million iPads in two and a half years (10/2012). Zero viruses on anything but jail-broken devices.

There are 775,000+ Apps available, controlled through the App-store. Over 40 BILLION application downloads.

Apple’s (Androids) system architecture protects the device from the laptop issues that require all the AV and firewalls to achieve any semblance of security – as long as the device isn’t Jail-broken (Rooted).

Do you Trust Apple/Android/Windows???

Apple – Yes. 100’s of millions sold, never an issue.
Android – Less than Yes. Had issues controlling their Store, open Source.
Windows – No. Not even safe with AV and firewalls.
What did the S+A Committee do? Support the FBI position that Apple and Android devices can be used, but only with Mobile Device Management Software (MDM). This can change the “user experience”, may require that you run your own App Store, but it does provide some Blackberry-like security services.

This allows only large, technically competent Law Enforcement agencies access to this technology and then at an additional cost – both for infrastructure and ongoing support.

**Status** – Policy changes reflecting the MDM requirement were passed by the APB and awaiting signature of the FBI Director.
Version 5.x of the CJIS Security Policy is much better than its predecessors, but we need to get away from the best-practices, check-list type security that is prevalent throughout the document.

A risk based CJIS security policy needs to be developed and deployed. The objective of a risk-based security program is not to provide remedies for every security breach or gap, but to delineate a comprehensive, systematic approach to risk mitigation and management.

Our systems will be safer, technology will be available faster to the officers on the street, money will be saved, information sharing across agencies will increase, and everyone will be safer.
A Rule based Policy Statement:

"No person shall access data that is classified at a level higher than their current role."

A Risk Based Policy Statement:

"Risks associated with data availability, confidentiality and integrity shall be classified by the business process owner and mitigated by adhering to templates, forms and documents that support the security process."
Paco’s Topic - Mobile ID

How to leverage installed systems
Interoperability- Image versus proprietary template
Accuracy – if it’s not accurate, who cares if it’s mobile!
Subject Acquisition Profiles or
  “Why are you taking the prints?”
Need to implement incremental enhancements to improve existing processes
Agnostic Mobile ID Devices

Mobile ID Devices

CSOs should not make recommendations on what mobile ID devices locals acquire, however, CSOs should require devices to adhere to national standards:

Interoperability – The state ID systems should only accept image-based searches – minutia-based searches should not be supported.

Accuracy – in order to ensure accuracy, systems should require images captured by the devices to generate a minimum NFIQ score of 7 in order to be processed.

Backward Compatibility – System should grandfather existing devices that meet the minimum FAP of 10 (as does the FBI for RISC).

Incremental quality improvement – Systems should establish threshold quality criteria for the acquisition of new equipment (i.e. FAP of 30 or greater for new devices).

Finger selection - Systems should support the type of searches needed – i.e. between 2 and 10 finger searches, depending on the purpose of the search. Some systems may want to support searches of only certain fingers (count and position - ex fingers 2 and 6 (index fingers). Systems should publish limitations so users will know before acquiring devices.
## Agnostic Mobile ID Devices

<table>
<thead>
<tr>
<th>Capture</th>
<th>5</th>
<th>10</th>
<th>20</th>
<th>30</th>
<th>40</th>
<th>45</th>
<th>50</th>
<th>60</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acquire flat images</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Acquire rolled images</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>No</td>
<td>Optional</td>
<td>Optional</td>
<td>Optional</td>
<td>Optional</td>
</tr>
<tr>
<td>Minimum resolution</td>
<td>500 ppi ± 10 ppi</td>
<td>500 ppi ± 10 ppi</td>
<td>500 ppi ± 10 ppi</td>
<td>500 ppi ± 10 ppi</td>
<td>500 ppi ± 5 ppi</td>
<td>500 ppi ± 5 ppi</td>
<td>500 ppi ± 5 ppi</td>
<td></td>
</tr>
<tr>
<td>Minimum Gray levels</td>
<td>256</td>
<td>256</td>
<td>256</td>
<td>256</td>
<td>256</td>
<td>256</td>
<td>256</td>
<td></td>
</tr>
<tr>
<td>Minimum Image Dimensions (w x h)</td>
<td>.5” x .65”</td>
<td>.5” x .65”</td>
<td>.6” x .8”</td>
<td>.8” x 1.0”</td>
<td>1.6” x 1.5”</td>
<td>1.6” x 1.5”</td>
<td>2.5” x 3.2”</td>
<td></td>
</tr>
<tr>
<td>Minimum image area</td>
<td>.325 sq in</td>
<td>.325 sq in</td>
<td>.48 sq in</td>
<td>.8 sq in</td>
<td>2.4 sq in</td>
<td>2.4 sq in</td>
<td>3.75 sq in</td>
<td>9.6 sq in</td>
</tr>
<tr>
<td>Compression algorithm</td>
<td>N/A</td>
<td>WSQ</td>
<td>WSQ</td>
<td>WSQ</td>
<td>WSQ</td>
<td>WSQ</td>
<td>WSQ</td>
<td></td>
</tr>
<tr>
<td>Maximum compression ratio</td>
<td>N/A</td>
<td>10:1</td>
<td>10:1</td>
<td>10:1</td>
<td>15:1</td>
<td>15:1</td>
<td>15:1</td>
<td></td>
</tr>
<tr>
<td>Simultaneous number of fingers</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1 to 2</td>
<td>1 to 2</td>
<td>1 to 3</td>
<td>1 to 4</td>
</tr>
<tr>
<td>Sensor certification</td>
<td>PIV</td>
<td>PIV</td>
<td>PIV</td>
<td>PIV</td>
<td>PIV</td>
<td>Appendix F</td>
<td>Appendix F</td>
<td>Appendix F</td>
</tr>
<tr>
<td>Minutiae extractor certification</td>
<td>PIV</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td>N/A</td>
<td></td>
</tr>
</tbody>
</table>

### Interchange

<table>
<thead>
<tr>
<th>Image / template</th>
<th>Minutiae</th>
<th>Image</th>
<th>Image</th>
<th>Image</th>
<th>Image</th>
<th>Image</th>
<th>Image</th>
<th>Image</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard used</td>
<td>INCITS 378-2004</td>
<td>ANSI/ NIST Type-4 or Type-14</td>
<td>ANSI/ NIST Type-4 or Type-14</td>
<td>ANSI/ NIST Type-4 or Type-14</td>
<td>ANSI/ NIST Type-4 or Type-14</td>
<td>ANSI/ NIST Type-4 or Type-14</td>
<td>ANSI/ NIST Type-4 or Type-14</td>
<td>ANSI/ NIST Type-4 or Type-14</td>
</tr>
</tbody>
</table>