



# **DOJ Endpoint Lifecycle Management System**

**Tivoli Endpoint Manager  
~BigFix**

**&**

**Continuous Monitoring**

**DOJ, Information Security Tools Team  
Oct, 2012**



# Agenda

- Continuous Monitoring – What is it?
- Concepts
- Implementation
  - Defining the problem
  - Implementing the solution
  - Lesson Learned
- Maturing the solution
- Metrics
- Conclusion



## "As Was" Technology Endpoint Monitoring and Management Capabilities

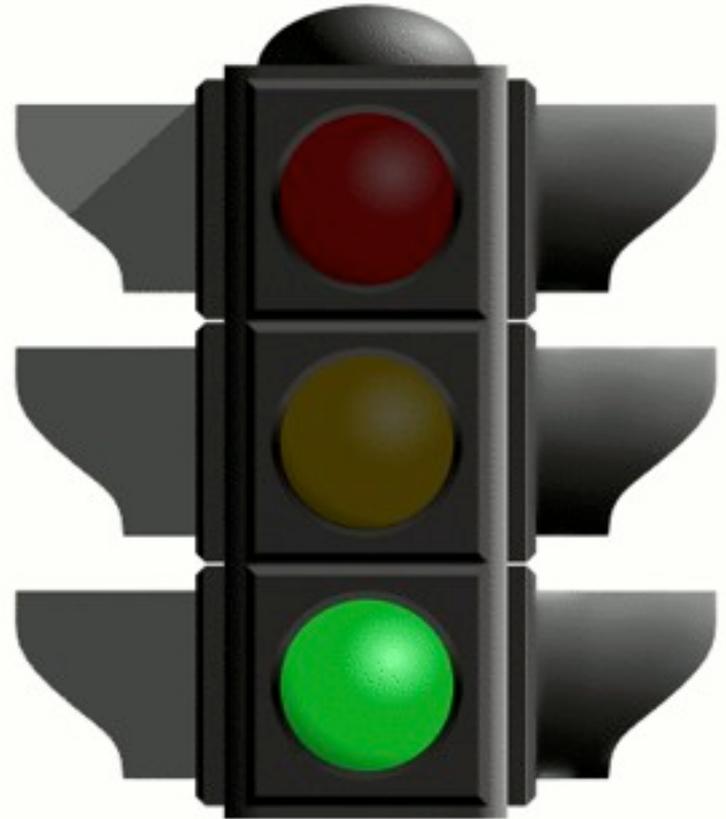
- Disconnected, autonomous tools
- Manual scans
- Manual reporting
- Manual re-entry
- Time consuming - telephone -tree data calls
- No enterprise view of 'front-end' risk



# Risk Scoring Decisions and Timeliness

On Sept. 17<sup>th</sup>, at 12:53 PM, the light was green at the intersection of State St. and N. Main St.

What does that data point tell us about the current moment?

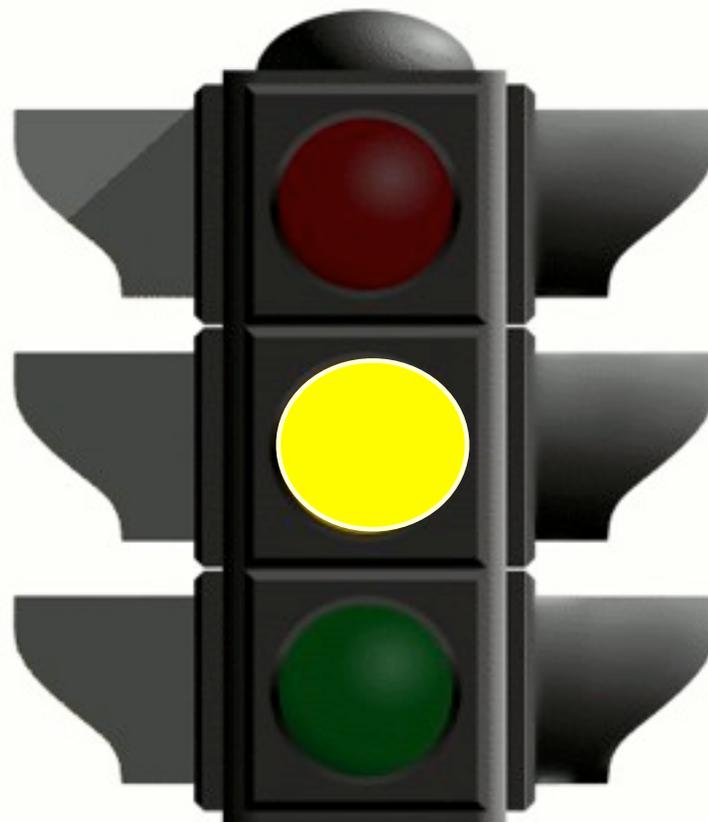




# Risk Scoring Decisions and Ambiguity/ Noise

On Sept. 18<sup>th</sup>, at 12:05 PM, the light was ??? at the intersection of State St. and N. Main St.

Do you have enough information to proceed?





# Background

- In 2010, as a follow-on to the demonstrated success of FDCC, OMB M-10-15 specified that:
- “Agencies should develop an enterprise-wide strategy for selecting subsets of their security controls to be monitored on an ongoing basis to ensure all controls are assessed during the three-year authorization cycle. A robust and effective continuous monitoring program will ensure important procedures included in an agency’s security authorization package (e.g., as described in system security plans, security assessment reports, and [Plans of Actions and Milestones] (POA&Ms)) are updated as appropriate and contain the necessary information for authorizing officials to make credible risk-based decisions regarding the security state of the information system on an ongoing basis. This will help make the security authorization process more dynamic and responsive to today’s federal missions and rapidly changing conditions.



**“Continuous monitoring is the backbone of true security.”**

Vivek Kundra, former Federal Chief Information Officer, Office of Management and Budget

**“If you can’t measure it, you can’t manage it.”**

Dr. W. Edwards Deming



# Continuous Monitoring

Information security continuous monitoring is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational **risk management** decisions. The objective is to conduct ongoing monitoring of the security of an organization's networks, information, and systems, and respond by accepting, avoiding/rejecting, transferring/sharing, or mitigating risk as situations change.

NIST SP 800-137 - Initial Public Draft



- To this point; lot's of talk about ConMon
- Not a word yet about automation!



# Continuous Monitoring and Automation

When possible, organizations look for automated solutions to lower costs, enhance efficiency, and improve the **reliability** of monitoring security-related information. Security is implemented through a combination of people, processes and technology. The automation of IT security deals primarily with automating aspects of security that require little human interaction. This includes items such as verifying technical settings on individual network endpoints, or ensuring that the software on a machine is up to date with organizational policy. This automation serves to augment the security processes conducted by security professionals within an organization.

NIST SP 800-137 pp. 15 – Initial Public Draft



# Business Needs

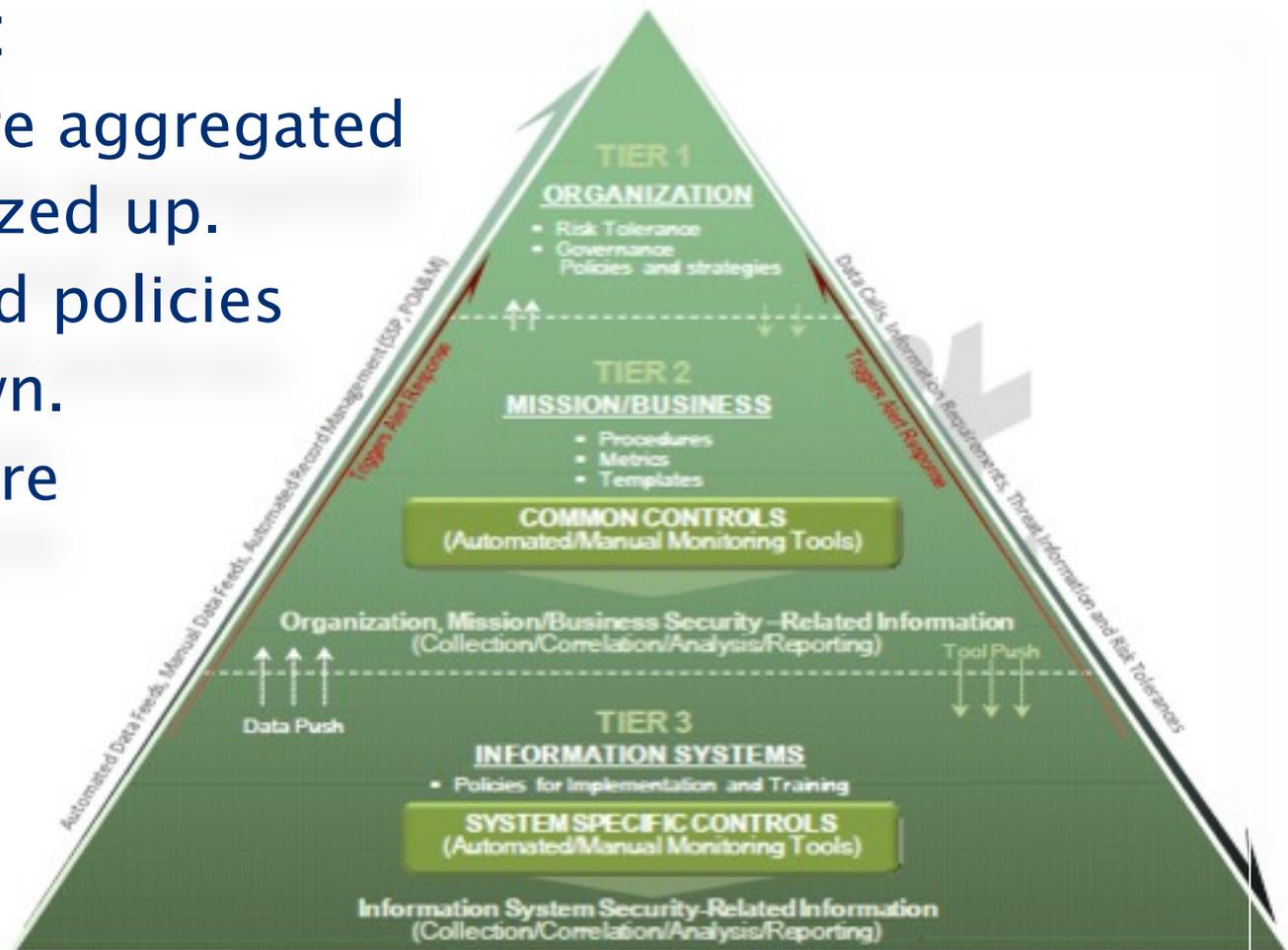
- Near real-time situational awareness
- Monitor trends in compliance
- Automate reporting
- Summarize data from multiple sources
- Reduce the units of work involved with compliance and accreditation



# Continuous Monitoring

## The Big Idea:

- Data feeds are aggregated and risk-analyzed up.
- Strategies and policies are issued down.
- Stove pipes are eliminated.
- Reporting is automated.





# Business Outcomes

- Visibility induces system operators to reduce risk
- Inspire competition
- Transparency prevents disputes
- Traceability motivates buy-In
- Configuration standardization reduces cost of ownership



# Continuous Monitoring

## Planning Notes:

- Define the Problem

- Perception operates on the basis of position
  - CFO, CIO, CTO, System Owner, Operations staff, and end-users will likely have different, valid, and sometimes competing concerns
- The way a problem is defined determines the possible solutions

- Plan the Solution

- If you have no plan – you have no control
  - How long will it take?
  - How much will it cost?
  - What must be done?

## Implementation Notes:

- Third party tools can each fulfill some roles for some subsystems.
- No tool currently exists to integrate all subsystems.
- Some development and customization is unavoidable – manage it.



# Lessons Learned

- Top-Down and Bottom-Up **Agile** approach to planning
  - BDUF (Big Design Up-Front) was seen as a risk to be avoided (too big to succeed)
  - Evolutionary SDLC planning approach
- Strong operational presence in design, implementation, requirements engineering, and early operations.
- Selling is a part of project management.
- Every exception or customization is a future blind-spot or development cost.



## "As IS" Technology Endpoint Monitoring and Management Capabilities

- 90% of Department endpoints under automated management
- Unified Management Platform
  - multiple platforms, one pane of glass for:
    - CVE, CCE, CPE
- Situational awareness in 'network-time'
- Diverse operational entities drinking the kool-aid:
  - Software asset management
  - Power management
  - Surveillance and inventory reports for data center consolidation
- Enterprise view of 'front-end' risk

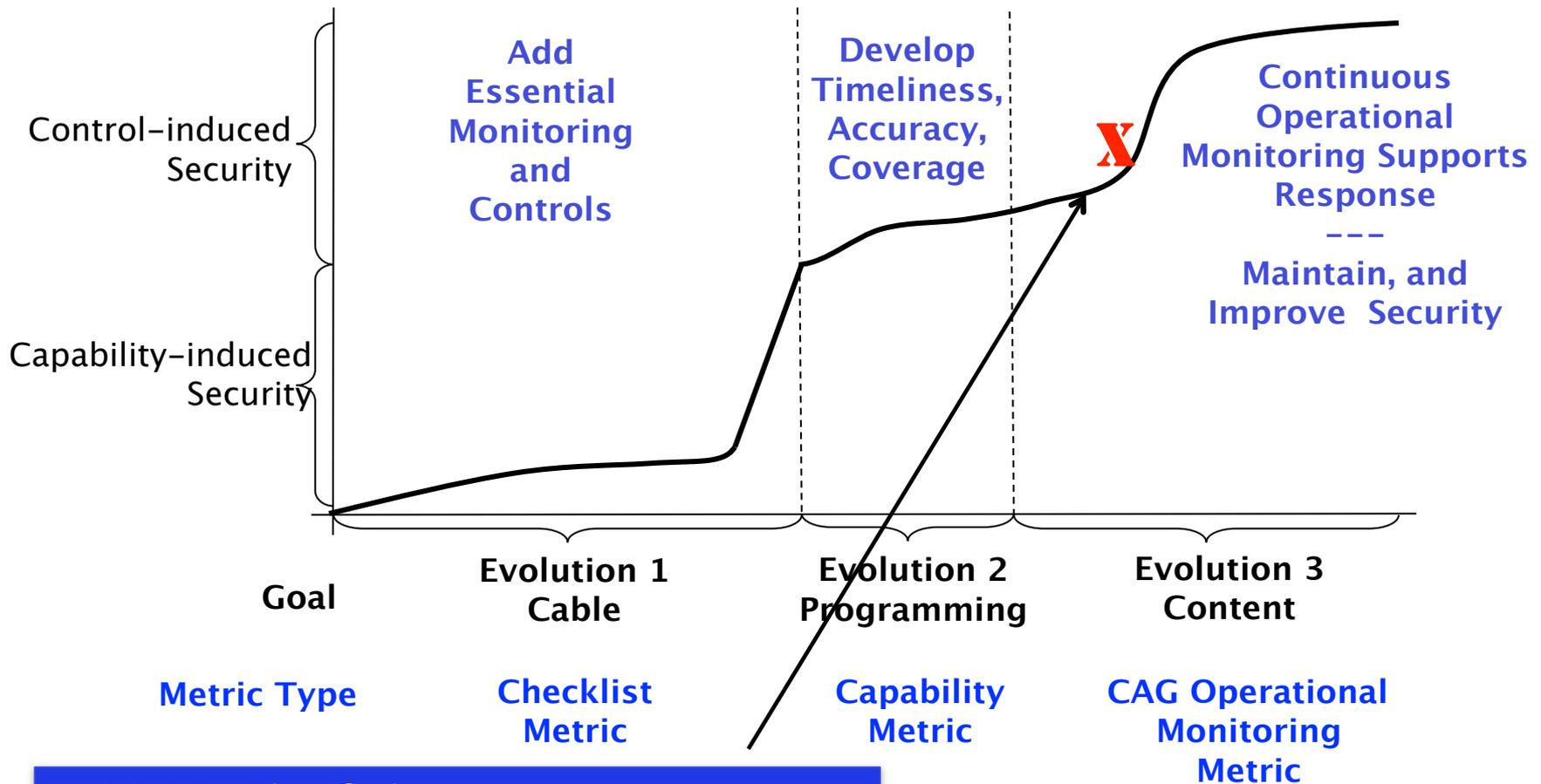


# Key Program Benefits

- A standardized platform and service delivery approach that enables improved communication and collaboration across the cyber-security workforce fostering and driving synergy and improved communication
- Standard security configurations that reduce attack surface and improve regulatory compliance across the Department;
- Enforcement of minimal desirable configurations throughout the DOJ enterprise resulting in fewer incidents;
- Configuration standardization resulting in a lower total cost of ownership per asset
- Increased efficiency and efficacy on security posture through collaboration and streamlining



# Continuous Monitoring Capability Maturity



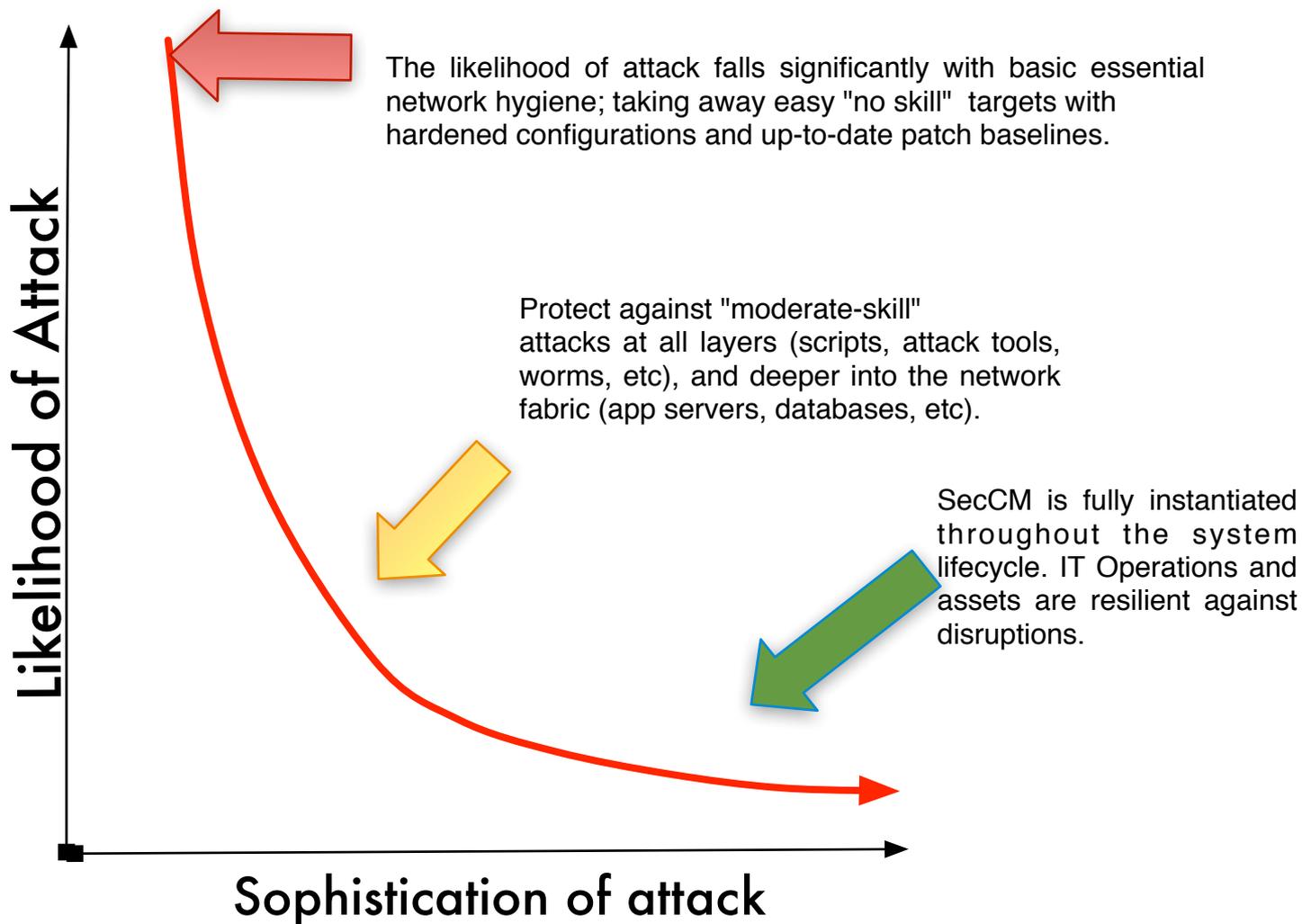
- Priorities identified
- Baselines established
- Measures available

Based on material developed by Kim Watson, NSA



# Maturity in Functional Terms

## Manage The Attack Surface

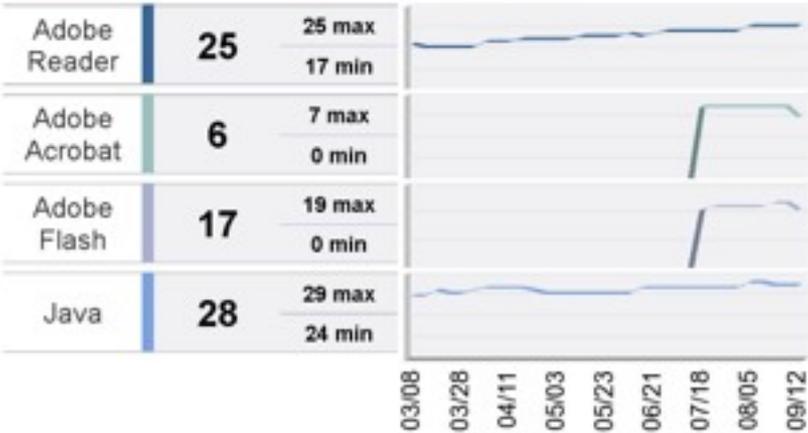




# Results

## Number of Installed Versions

CM-02, CM-02(5) Baseline Configuration\*  
 CM-08, CM-08(1), CM-08(2) Information System Inventory\*



## Antivirus DAT Files

SI-03, SI-03(1), SI-03(2) Malicious Code Protection\*  
 SI-04 Information System Monitoring\*

DAT Age in days Aug 1, 2011 to Sep 26, 2011



No AV Product or w/ Outdated DAT File	Count
<b>No AV Product or w/ Outdated DAT File</b>	<b>41 assets</b>
eTrust	N/A
Forefront	N/A
McAfee	2
Symantec	N/A
Trend Micro	N/A



# Conclusion

## •Questions /Comments

### •For more information contact

- ✓ *Kevin.Cox@USDOJ.GOV*
- ✓ *David.Otto@USDOJ.GOV*