Transforming Federal Cyber Security Management

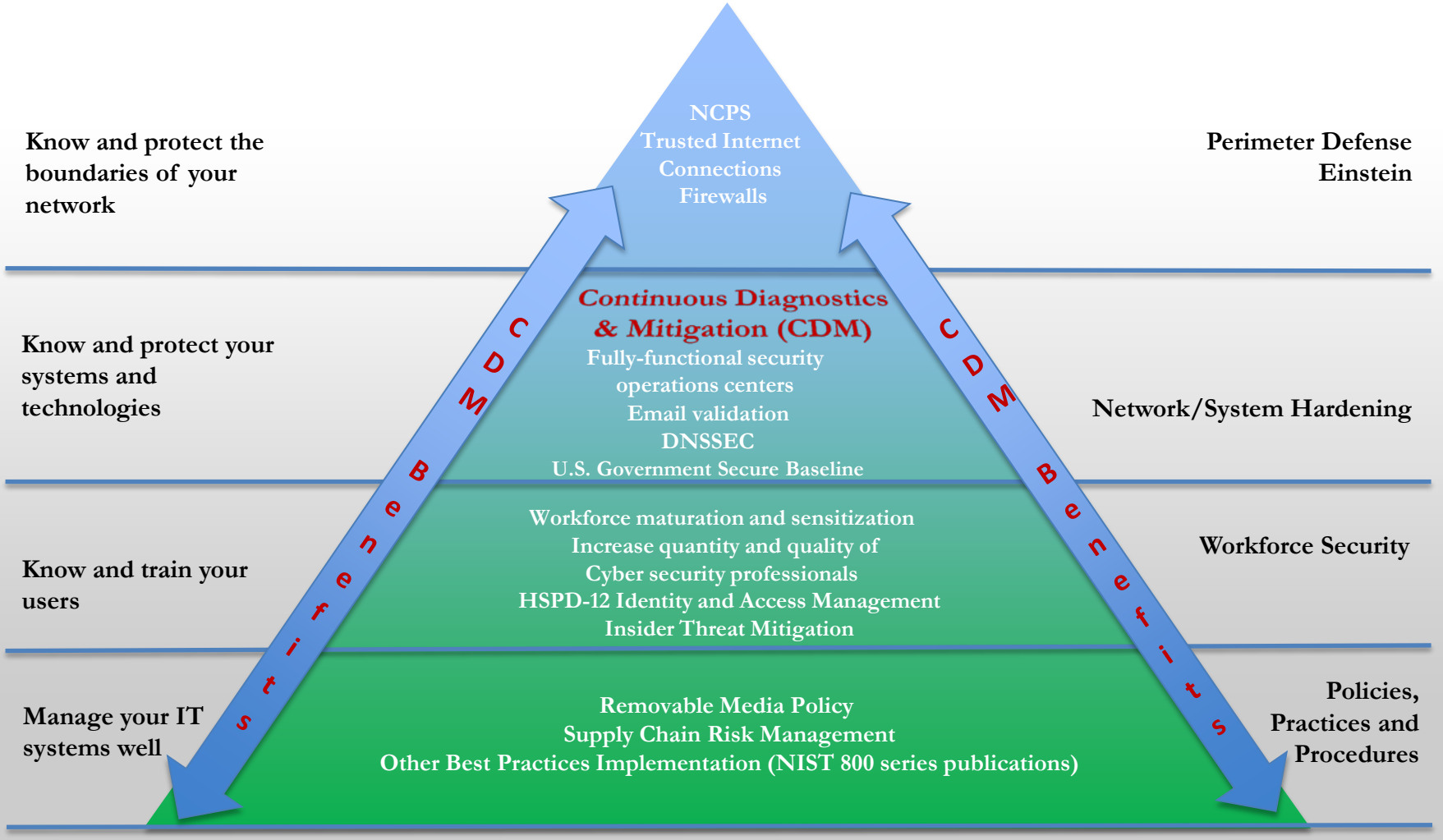
June 12, 2013

Outline

1. Securing .gov
2. Why CDM[1]?
   a. What is the Problem?
   b. Current Fix…
      - …And the Results
   c. Proposed Alternative
      - How will CDM Work?
      - How will Continuous Authority to Operate support CDM?
      - Expected Benefits
      - Cost
      - Timelines
3. Next Steps

[1] Continuous Diagnosis and Monitoring

Securing .gov



Why CDM?

Why CDM?

A recent report from CSIS[2] found that CDM stops 85% of cyber attacks by:

- Searching for, finding, fixing, and reporting the worst cyber problems first in near-real time

- It will also:
  - Enable System Administrators to:
    - Respond to exploits at network speed
    - Fulfill A-130 responsibilities as intended
    - Implement NIST Publications on Continuous Monitoring (800-137 and parts of 800-37)
  - Use strategic sourcing to lower cost

[2] James A. Lewis, *Raising the Bar for Cybersecurity*. Washington, DC: CSIS, 2013.

Why CDM? (Cont.)

According to the CSIS report:

- 75% of the attacks use known vulnerabilities that could be patched;
- More than 90% of successful attacks require only the most basic techniques; and,
- **96%** of successful breaches **can be avoided** if the victim puts in place simple or intermediate controls.

What is the Problem?

Every Three Days (on federal networks):

- Trillions of cyber events
- Billions of potentially defective hardware, software, and account changes
- Millions of attempted attacks at internet speed
- Thousands of new flaws introduced
- Hundreds of attacks that succeed

Every Three Months:

- Over 10,000 successful attacks
- An unknown number of these attacks are repaired
- Terabytes of data are stolen
- Over 7,200 reports are written[3]
- Hundreds of labor hours are wasted

Every Three Years:

- Thousands of assessments and other reports are written and issued. Each:
  - Requires 3 to 9 months to prepare;
  - Is out of date the moment it is printed; and,
  - Provides only a snapshot in time vs. real-time identification and mitigation of problems.

[3] Office of Management and Budget, *Memorandum 02-01: Guidance for Preparing and Submitting Security Plans of Action and Milestones*. Washington, DC: OMB, 2001.

Current Fix…

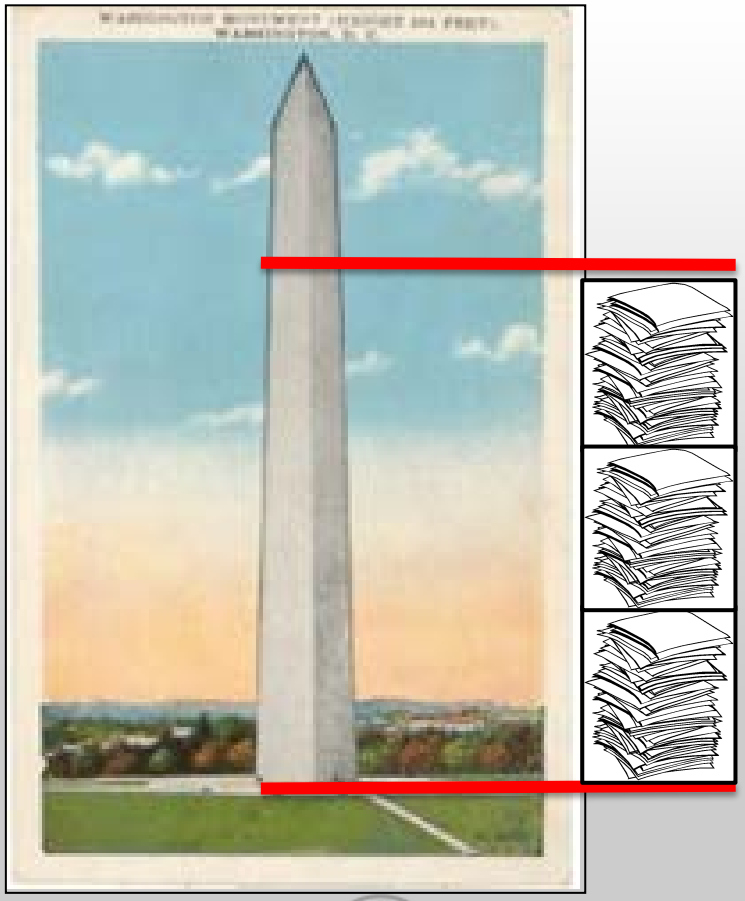
Short answer: Plans, Reports, and Manual Audits

- 3-month to 3-year remediation plans[4]
- Triennial reports currently required by regulation
- Manual audit and oversight

[4] Office of Management and Budget, *Circular A-130, Appendix III: Security of Federal Automated Information Resources*, Washington, DC: OMB, 2000

…the Results

We estimate that these manual plans, reports, and audits cost between $600M and $1.9B a year, at a cost of $1,400 per page



438 feet of cyber paperwork generated and filed (based upon $1.9B spent)

In Other Words…

In large civilian agencies, paperwork accounts for as much as 65% of the overall IT Security effort

Encompassing:

- Manual Audits
- Manual Plan of Action reports
- Manual Cyber Scope reporting
- Manual Annual Testing
- FISMA portion of financial statement

…Our current approach is:

Unresponsive

Uneconomical

Unsustainable

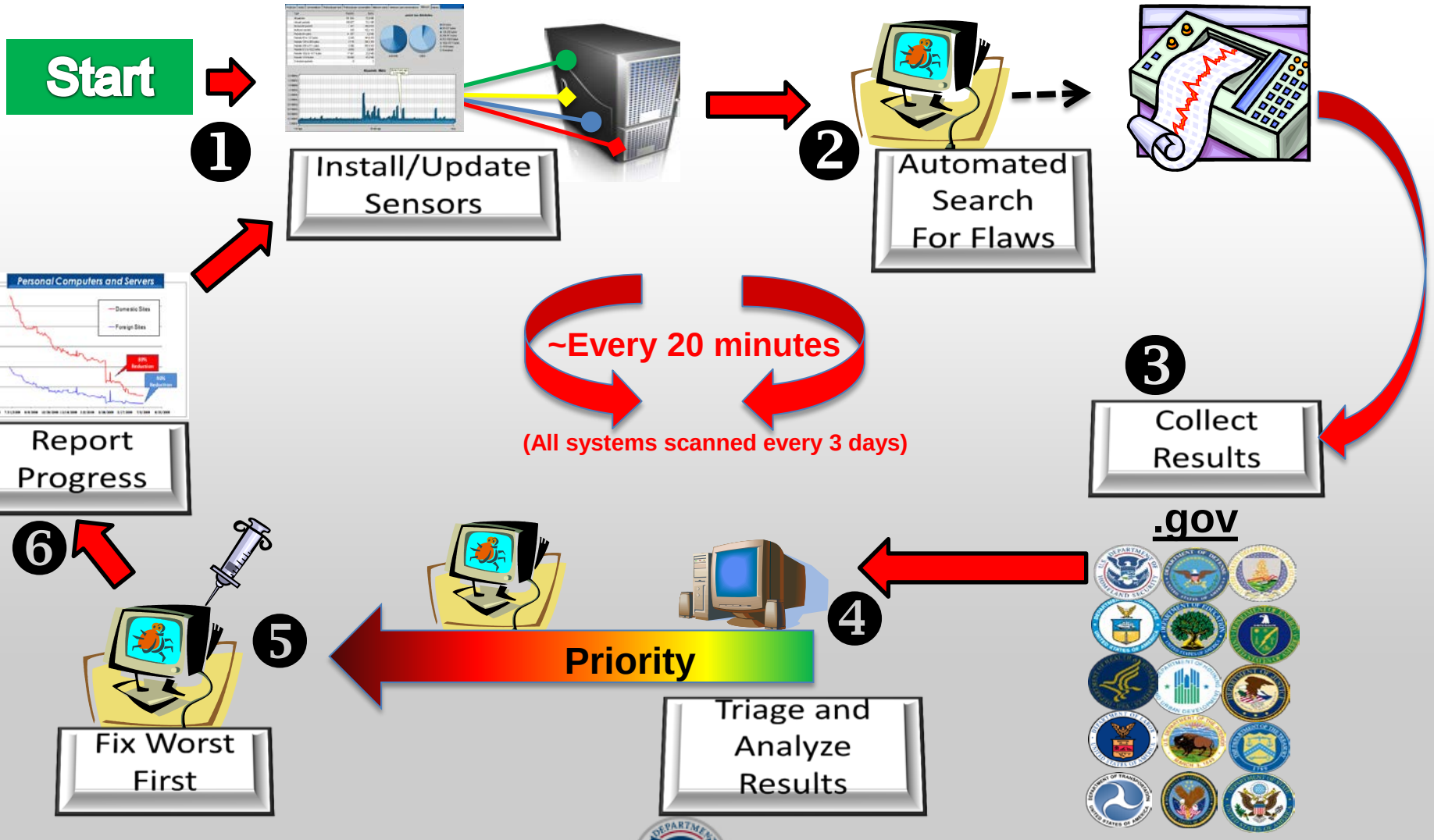
Proposed Alternative

Short Answer: Automate control testing and progress tracking.

This approach will:

- Provide near real time results
- Fix the worst problems first
- Accelerate defense through faster updates on attacks and methods
- Enable defenders to identify and mitigate flaws at network speed

How will CDM work?



How will we get there?

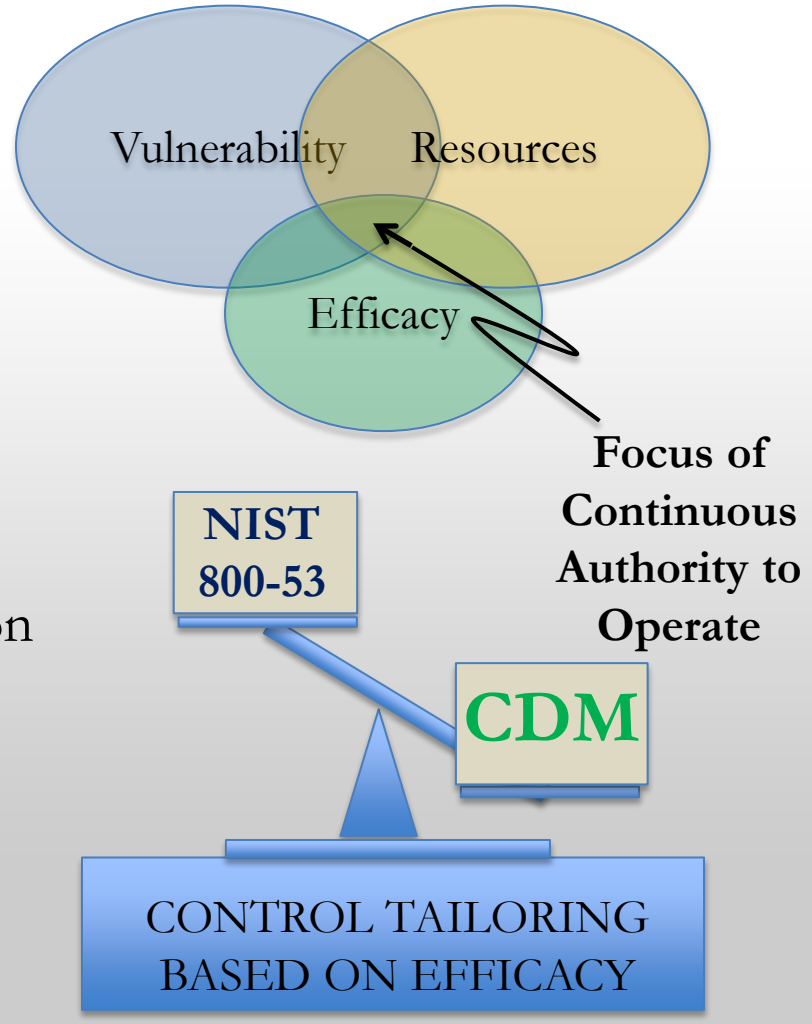
- Redirecting resources, time, and expertise away from plans and reports
- Automate the Authority to Operate (ATO)

How will Automated (Continuous) ATO support CDM?

- Enables prioritization of the most urgent controls by risk executives
- Clarifies standards for IG assessment
- Replaces tri-annual re-authorization with ongoing validation cycle

How does Automated (Continuous) ATO work?

1. Verify risk categorization
2. Prioritize selection of controls based upon vulnerability, resources, and efficacy
3. Develop a security plan
4. Grant authority to operate based upon existing security posture and plan
5. Implement and monitor selected controls
6. Repeat as required



Expected Benefits

- All systems tested every 3 days vs. every 3 years
- Worst problems identified in minutes vs. years
- Worst problems fixed in days vs. months
- CDM will cost $200m vs. $600m per year and will use 6% vs. 18%-65% of each .gov cybersecurity dollar

Next Steps

Next Steps

1. Adopt an Administration policy to convert from manual cyber security practices toward automated CDM NLT than beginning of FY 2014 (Leads: OMB, NIST, DHS)
2. Immediately issue an OMB memorandum to:
   a. Interpret existing regulations to implement automated CDM
   b. Designate CDM strategic sourcing vehicles as "first choice contracts"
   c. Modify OMB FISMA and Cyber Scope reporting requirements
   d. Establish ongoing mechanism to coordinate CDM policy and operations
3. Work with GAO to update audit standards to oversee CDM initiative (Leads: OMB, DHS, GAO, OIGs)

Background Slides

OMB A130 Appendix III

Under the "controls for general support systems" section:

- Review of Security Controls. Review the security controls in each system when significant modifications are made to the system, but at least every three years. The scope and frequency of the review should be commensurate with the acceptable level of risk for the system. Depending on the potential risk and magnitude of harm that could occur, consider identifying a deficiency pursuant to OMB Circular No. A-123, "Management Accountability and Control" and the Federal Managers' Financial Integrity Act (FMFIA), if there is no assignment of security responsibility, no security plan, or no authorization to process for a system.
- Authorize Processing. Ensure that a management official authorizes in writing the use of each general support system based on implementation of its security plan before beginning or significantly changing processing in the system. Use of the system shall be re-authorized at least every three years.

Under the "controls for major applications" section:

- Review of Application Controls. Perform an independent review or audit of the security controls in each application at least every three years. Consider identifying a deficiency pursuant to OMB Circular No. A-123, "Management Accountability and Control" and the Federal Managers' Financial Integrity Act if there is no assignment of responsibility for security, no security plan, or no authorization to process for the application.
- Authorize Processing. Ensure that a management official authorizes in writing use of the application by confirming that its security plan as implemented adequately secures the application. Results of the most recent review or audit of controls shall be a factor in management authorizations. The application must be authorized prior to operating and re-authorized at least every three years thereafter. Management authorization implies accepting the risk of each system used by the application.

Under the "Descriptive Information" section:

- Review of Security Controls. The security of a system will degrade over time, as the technology evolves and as people and procedures change. Reviews should assure that management, operational, personnel, and technical controls are functioning effectively. Security controls may be reviewed by an independent audit or a self review. The type and rigor of review or audit should be commensurate with the acceptable level of risk that is established in the rules for the system and the likelihood of learning useful information to improve security. Technical tools such as virus scanners, vulnerability assessment products (which look for known security problems, configuration errors, and the installation of the latest patches), and penetration testing can assist in the on-going review of different facets of systems. However, these tools are no substitute for a formal management review at least every three years. Indeed, for some high-risk systems with rapidly changing technology, three years will be too long…