CONTINUOUS MONITORING AND ITS ABILITY TO CREATE EFFICIENCIES

REDUCTION OF REPORTING WHEREVER POSSIBLE

Earl Crane, PhD

Director for Federal Cybersecurity

National Security Staff, The White House

THE QUESTION

- Are we more secure today than yesterday? (POTUS)
  - Hard to measure
    - We don’t know if we are getting more secure
  - Hard to meet
    - We don’t know how much we need to be secure
  - Hard to manage
    - We don’t have good reliable models of what is cost effective security

“If you can not measure it, you can not improve it.”
– Lord William Thomson Kelvin

THE ANSWER(S)

- …Tend to fall to the lowest common denominator
  - Fear, Uncertainty, and Doubt
  - Compliance-based security
  - Auditor-driven security
  - Pain-based security
  - Return/Annualized loss based security

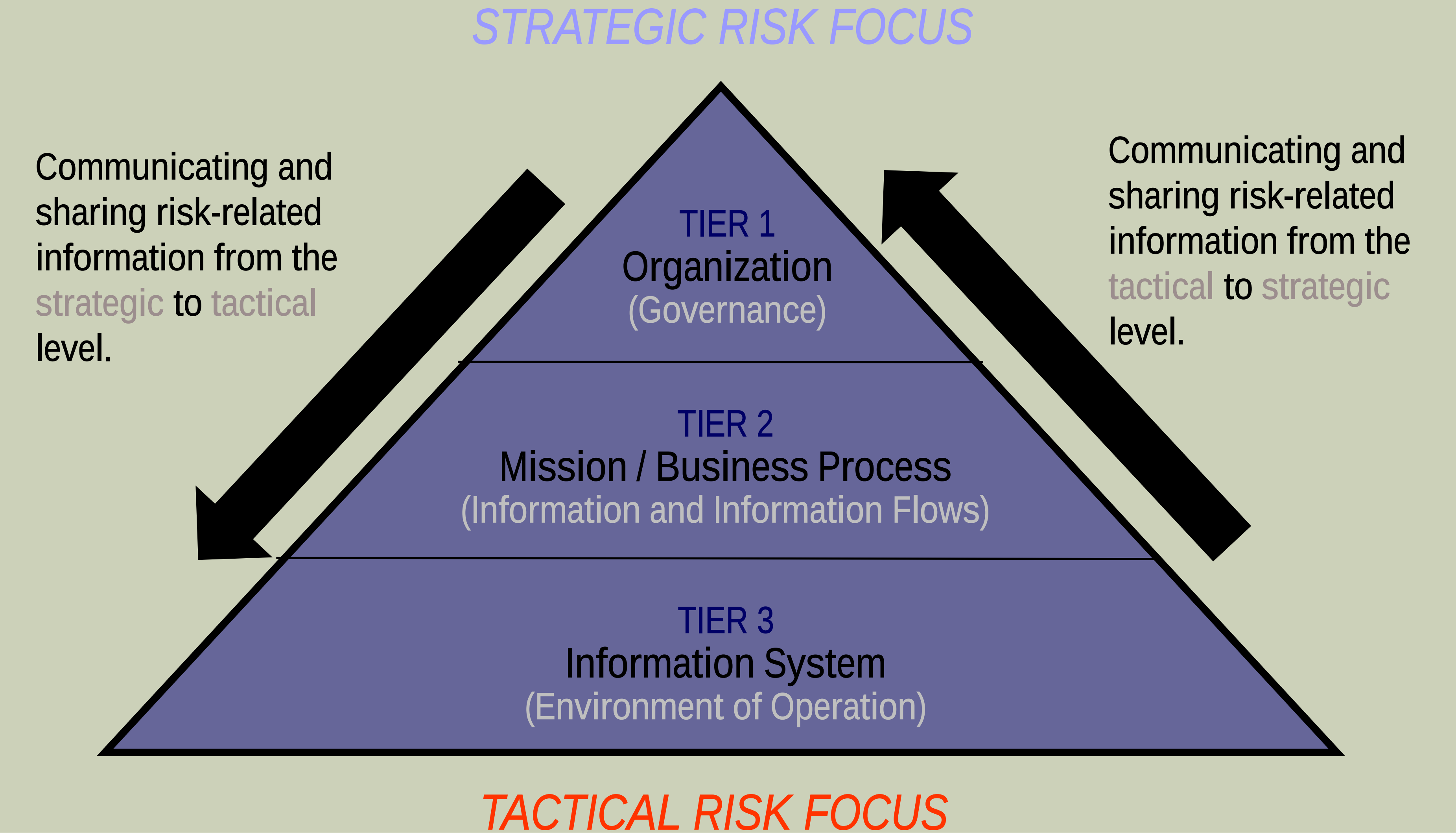
THE (BETTER) ANSWER(S)…

- Security is the means to enable the mission, not the mission objective
  - Need to focus on mission objectives, not “if we are more secure today than yesterday”
  - The mission gets lost in the quest for compliance
  - This is lost on many CISOs, auditors, regulatory bodies
- The purpose:
  - Enabling the mission
  - Focus on business impact and value generation
  - Consequence management and loss mitigation
- The best security is transparent security
  - “Security need not be obtrusive, obvious, or restrictive to be effective”

SECURITY MANAGEMENT THEORY

- Prioritize
  - Set priorities - if everything is the priority, nothing is the priority
  - Not all threats, vulnerabilities, and assets are equal
  - Focus limited resources on most cost effective controls
- Minimize
  - Not all missions are equal
  - Varies based on mission requirements for confidentiality, integrity, availability
- Specialize
  - Know your capabilities and environment, know your threat actor
  - Target high risk/frequency threats like spear phishing, exfiltration
  - Tailor your security program specific to mission and business functions

NIST RISK MANAGEMENT FRAMEWORK SP800-39



STRATEGIC RISK FOCUS

Communicating and sharing risk-related information from the strategic to tactical level.

TIER 1
Organization
(Governance)

TIER 2
Mission / Business Process
(Information and Information Flows)

TIER 3
Information System
(Environment of Operation)

Communicating and sharing risk-related information from the tactical to strategic level.

TACTICAL RISK FOCUS

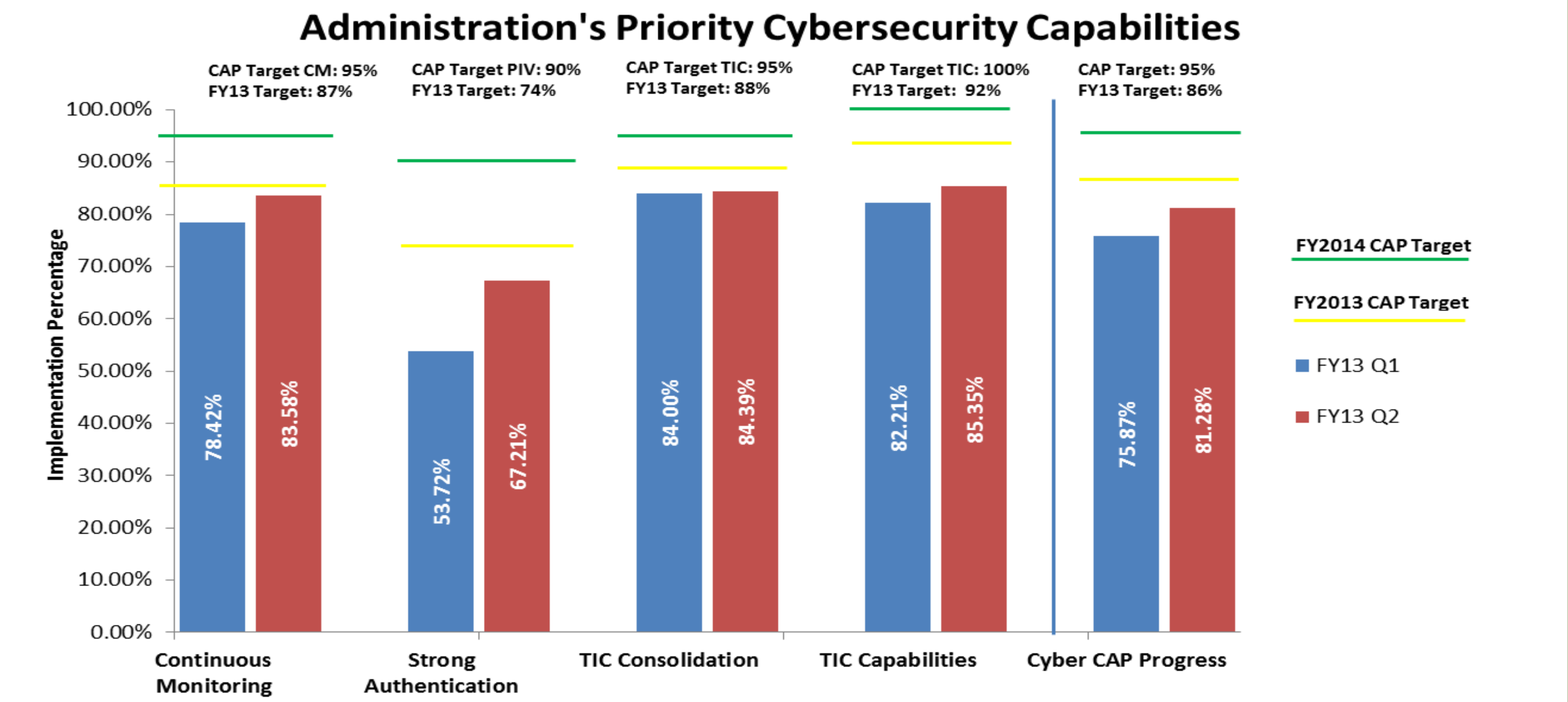
FEDERAL INFORMATION SECURITY MANAGEMENT PRIORITIES

Prioritize

- The priority is to know *what data and information is entering and exiting my networks, what components are on my information networks and when my security status changes,* and *who is on my systems*.

- The Administration’s priority cybersecurity capabilities are:
  1. Trusted Internet Connections (TIC)
  2. Continuous Monitoring of Federal Information Systems
  3. Strong Authentication

CAPABILITY ADOPTION FY2013Q2



PRIORITIZE: VULNERABILITY MANAGEMENT

- Selecting the “right” control to is a misnomer
  - This is compliance-focused security management
  - NIST 800-53 R4 increases controls in the catalog, but provides guidance to customize security plans with risk-based control selection
- Focus has frequently been on controls
  - Sans Top 20, Consensus Audit Guidelines
  - Control implementation verification
- Focus on the capability not the control
  - First identify the end state, then define capabilities
  - Does the capability produce the desired effect
  - Do the outcomes and results meet the capability objectives?

FEDERAL INFORMATION SECURITY MANAGEMENT GOALS

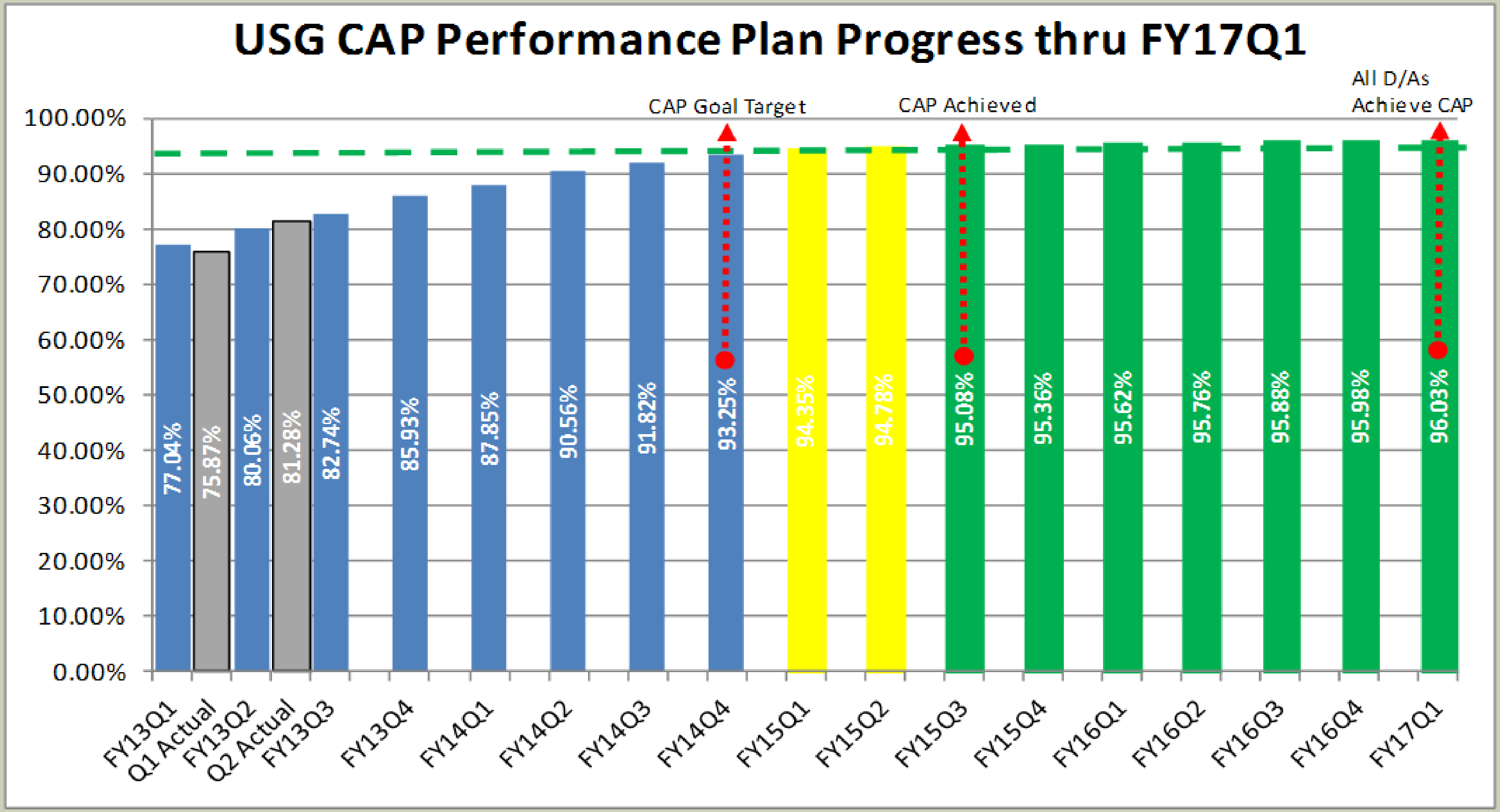
Minimize

- Reduce unnecessary efforts
  - Migrate towards automated metrics
  - Focus on what is most important first
  - Eliminate duplicate security programs, practices, and capabilities
- Improve visibility
  - Continuous monitoring and sharing current cybersecurity posture
  - Enhance visibility of posture and threats to the Federal IT environment

Specialize

- Improve accountability
  - To the Chief Operating Officer / Deputy Secretary, the Performance Improvement Officer (PIO) and mission owner
  - Through department quarterly and annual measurement
- Mature the measurement of information security management
  - Measure success past the checklist

CAPABILITY ADOPTION THRU FY17Q1



MEASURING SUCCESS - CYBERSECURITY PERFORMANCE MANAGEMENT

- Performance Management
  - Use repeatable and standardized metrics, automating whenever possible
  - Maintain independence and automation
  - Integrate security as part of regular performance management reviews, considering cost, schedule, and performance tradeoffs from a risk-based perspective
- Progression of measurement
  - Compliance based metrics
  - Risk based metrics
  - Outcome based metrics
  - Maturity based metrics
- USG objective: Progress past compliance-based by defining risk management by objectives and targeted outcomes

PERFORMANCE MANAGEMENT TO MEASURE OUTCOMES

- Challenge of measuring capabilities and outcomes

Administration Performance Area	Annual FISMA Metric Section	Performance Metric	Minimal Level	Target Level
Continuous Monitoring – Assets	2.2	% of assets in 2.1, where an automated capability (device discovery process) provides visibility at the organization's enterprise level into asset inventory information for all hardware assets.	80%	95%
Continuous Monitoring – Configurations	3.1.3	% of the applicable hardware assets (per question 2.1), of each kind of operating system software in 3.1, has an automated capability to identify deviations from the approved configuration baselines identified in 3.1.1 and provide visibility at the organization's enterprise level.		
Continuous Monitoring – Vulnerabilities	4.2	% of hardware assets identified in section 2.1 that are evaluated using an automated capability that identifies NIST National Vulnerability Database vulnerabilities (CVEs) present with visibility at the organization's enterprise level.		
Strong Authentication - Identity Management HSPD-12	5.2.5, 5.4.5 &10.2.5	% of ALL people required to use Personal Identity Verification (PIV) Card to authenticate.	50%	75%
TIC Consolidation - CNCI #1	7.2	% of external network traffic passing through a Trusted Internet Connection (TIC).	80%	95%
TIC Capabilities - CNCI #1 & #2	7.1	% of required TIC capabilities implemented by TIC(s) used by the organization.	95%	100%

REDUCTION OF REPORTING WHEREVER POSSIBLE

- Prioritize - on capabilities
- Minimize - unnecessary efforts, lack of visibility
- Specialize - Accountability to the right people, beyond the checklist

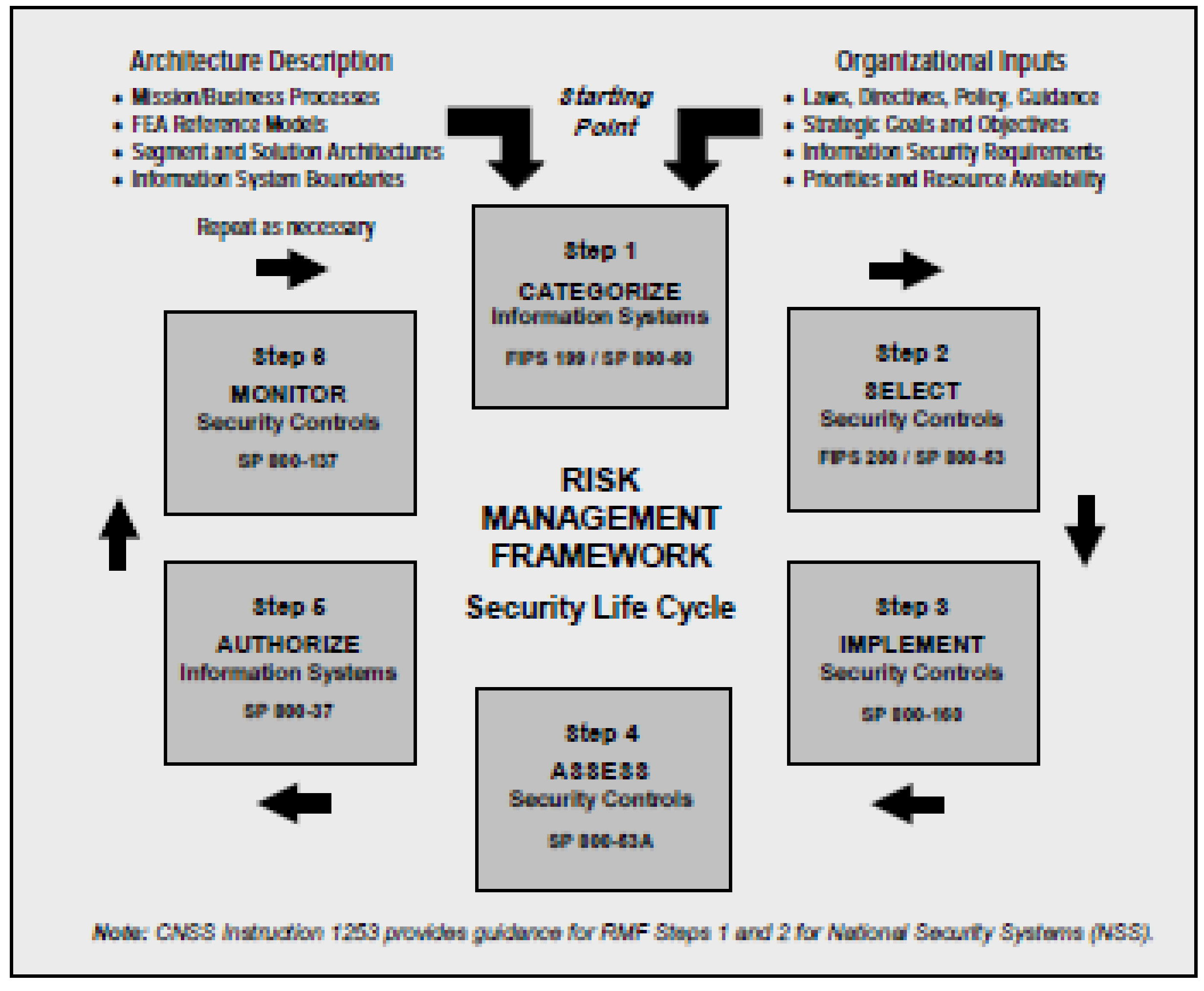
Questions?

Earl Crane, PhD

ecrane@nss.eop.gov

BACKUP

NIST RISK MANAGEMENT FRAMEWORK SP 800-39



Architecture Description

- Mission/Business Processes
- FEA Reference Models
- Segment and Solution Architectures
- Information System Boundaries

Starting Point

Organizational Inputs

- Laws, Directives, Policy, Guidance
- Strategic Goals and Objectives
- Information Security Requirements
- Priorities and Resource Availability

Repeat as necessary

Step 1
CATEGORIZE
Information Systems
FIPS 199 / SP 800-60

Step 2
SELECT
Security Controls
FIPS 200 / SP 800-53

Step 3
IMPLEMENT
Security Controls
SP 800-160

Step 4
ASSESS
Security Controls
SP 800-53A

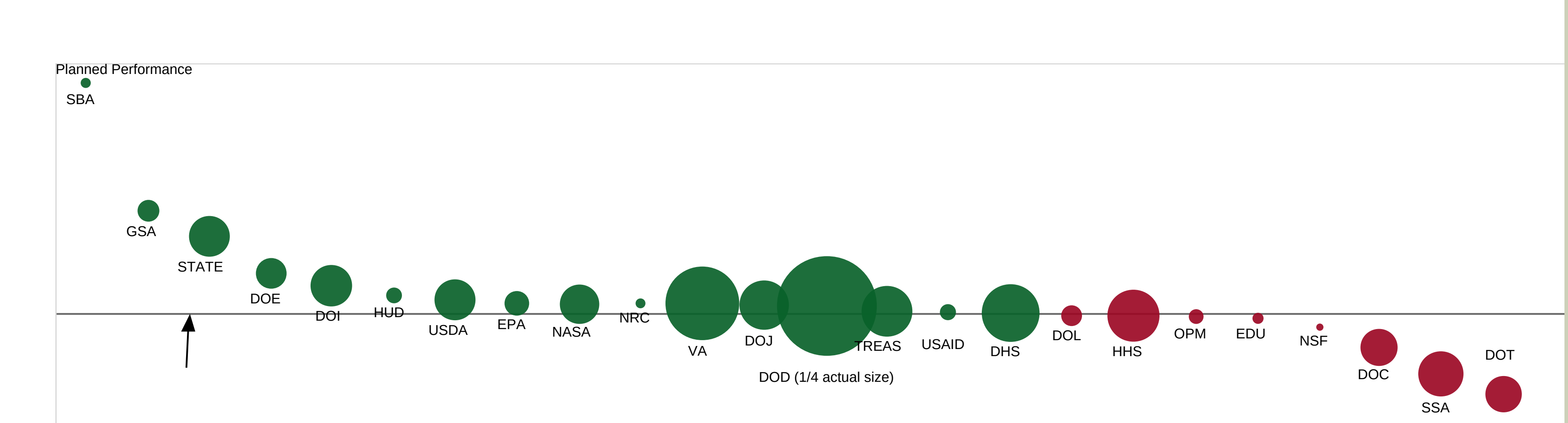
Step 5
AUTHORIZE
Information Systems
SP 800-37

Step 6
MONITOR
Security Controls
SP 800-137

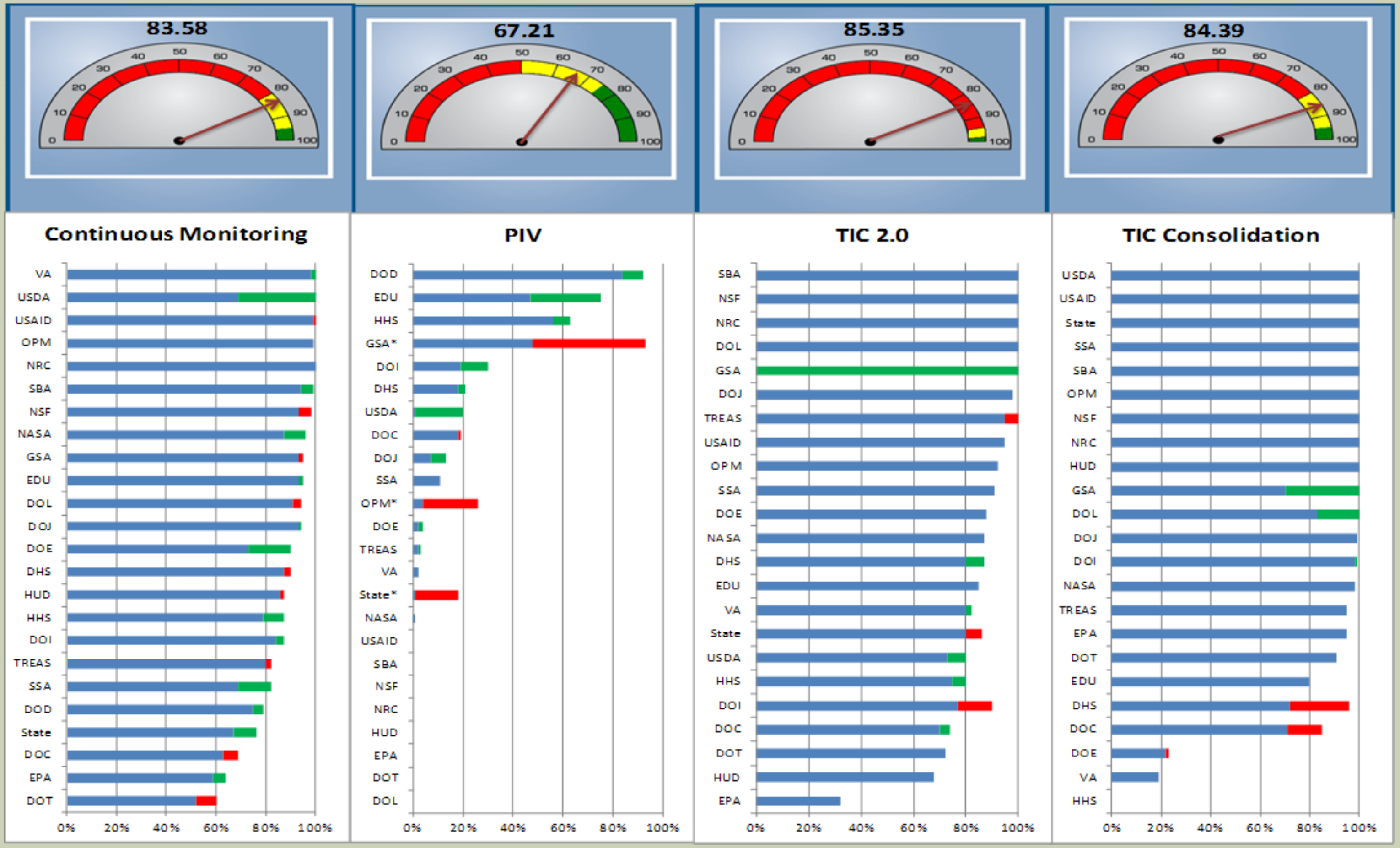
RISK
MANAGEMENT
FRAMEWORK
Security Life Cycle

Note: CNSS Instruction 1253 provides guidance for RMF Steps 1 and 2 for National Security Systems (NSS).

FEDERAL DEPARTMENT AND AGENCIES ABOVE AND BELOW PERFORMANCE PLAN FOR FY2013 Q2



FEDERAL DEPARTMENT AND AGENCY PERFORMANCE FOR FY2013 Q1 – Q2


Continuous Monitoring
VA
USDA
USAID
OPM
NRC
SBA
NSF
NASA
GSA
EDU
DOL
DOJ
DOE
DHS
HUD
HHS
DOI
TREAS
SSA
DOD
State
DOC
EPA
DOT
PIV
DOD
EDU
HHS
GSA*
DOI
DHS
USDA
DOC
DOJ
SSA
OPM*
DOE
TREAS
VA
State*
NASA
USAID
SBA
NSF
NRC
HUD
EPA
DOT
DOL
TIC 2.0
SBA
NSF
NRC
DOL
GSA
DOJ
TREAS
USAID
OPM
SSA
DOE
NASA
DHS
EDU
VA
State
USDA
HHS
DOI
DOC
DOT
HUD
EPA
TIC Consolidation
USDA
USAID
State
SSA
SBA
OPM
NSF
NRC
HUD
GSA
DOL
DOJ
DOI
NASA
TREAS
EPA
DOT
EDU
DHS
DOC
DOE
VA
HHS