Information Security Continuous Monitoring (ISCM) Program Evaluation

Cybersecurity Assurance Branch
Federal Network Resilience Division

Chad J. Baer
FNR Program Manager
Chief Operational Assurance

Homeland Security

Introduction

- **Chad J. Baer, Chief Operational Assurance**
  - Cybersecurity Assurance Branch, Federal Network Resilience
- **NCCoE tasked in three areas to support Federal Network Resilience**
  - Task #1 – Develop Information Security Continuous Monitoring Assessment Methodology
    - NCCoE will develop a methodology to assess federal agency ISCM programs. The methodology will be based on a staff assistance approach as opposed to a more traditional compliance based approach.
  - Ron Rudman, Senior Principal Cybersecurity Engineer
- **Get out of the Audit mindset for this presentation!**

Homeland Security

Agenda

- INTRODUCTION
- FEDERAL NETWORK RESILIENCE
- CYBERSECURITY ASSURANCE BRANCH ASSISTANCE
- FEDERAL ISCM EVALUTION

Homeland Security

Federal Network Resilience

A brief overview of the FNR mission and organizational goals

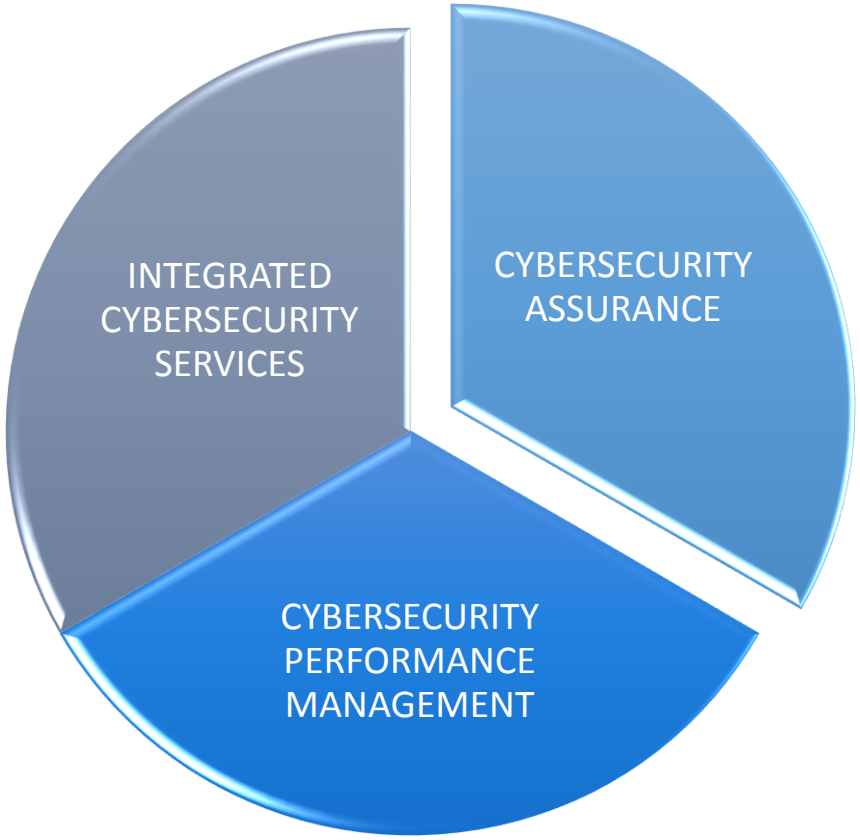
Federal Cybersecurity Priorities and Drivers

- **FISMA 2014 Authorities**
  - The Secretary of DHS, in consultation with the Director of OMB, shall administer the implementation of agency information security policies and practices for information systems:
    - "monitoring agency implementation of information security policies and practices"
    - "providing operational and technical assistance to agencies in implementing policies, principles, standards, and guidelines on information security, including ***implementation of standards promulgated under section 11331 of title 40"***
  - ***Supports Federal Agencies mission in meeting responsibilities under Section 3554***
- **Administration Cross-Agency Priority Goals (FY15-17)**
  - Information Security Continuous Monitoring Mitigation (ISCM) – *Provide ongoing observation, assessment, analysis, and diagnosis of an organization's cybersecurity: posture, hygiene, and operational readiness*
- ***OMB Memorandum 14-03 – Enhancing the Security of Federal Information and Information Systems***

Homeland Security

FNR Mission Goals

- Improve Federal cybersecurity
- Develop measureable cybersecurity performance metrics
- Engage with agencies across the Executive Branch to support priority cybersecurity programs



Homeland Security

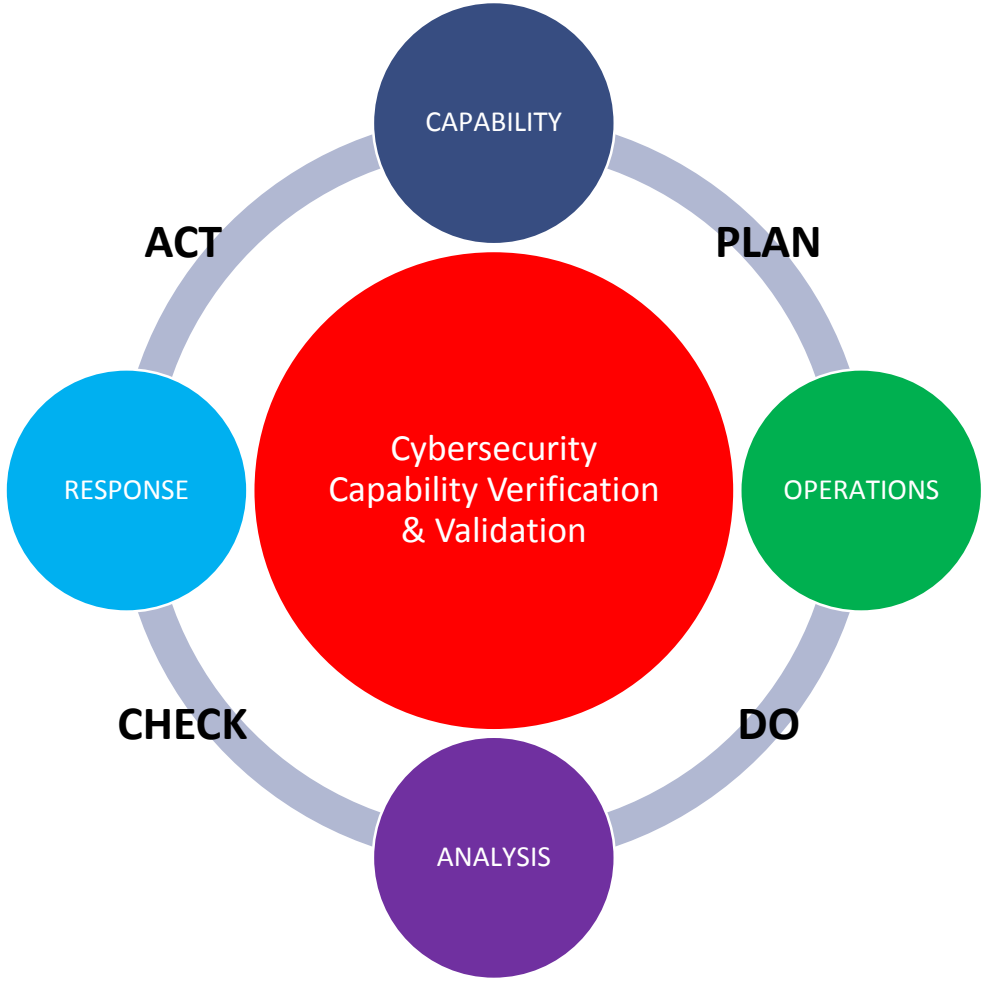
Cybersecurity Assurance Branch Goals

- Deploy ***adaptive*** cybersecurity assessments of federal civilian agency systems to validate current state cybersecurity against critical federal cybersecurity initiatives, and improve agency and federal cybersecurity posture.
- Provide ***continuous*** assistance to agencies by engaging in security engineering and solution support efforts to verify implementation of security controls, review security architecture, and help define critical systems; to ensure good quality data collection and integration of all priority Federal cybersecurity programs.
- Provide a ***holistic*** view of Federal cybersecurity posture, and show agencies are improving!

Homeland Security

Operational Assurance & Readiness

- ***Capability*** **–** Does the agency have a capability adopted and defined?
- ***Operations*** **–** Are they meeting those capabilities functionally in operations?
- ***Analysis*** **–** Do they collect and understand data outputs?
- ***Response*** **–** Does the agency use this information to improve their capabilities, operations, and analysis?



Homeland Security

Operational Assurance Services

- **Federal Incident Response Evaluation –** Based off the Federal Computer Network Defense (F-CND) assessment developed by FNR, US-CERT, and SEI. Added DISA Evaluator's Scoring Metrics (ESM) and priority levels.
  - This is a robust evaluation of incident management **capabilities** that can facilitate an initial triage of IR/IH program implementation. This is not a verification of operational execution.

✓ **Federal ISCM Evaluation –** A modular evaluation which initially leverage NIST SP 800-137 Information Security Continuous Monitoring guidance and the US Government Concept of Operations for ISCM to provide a holistic view of D/A cybersecurity based on ISCM domains.
  - Validates ISCM implementations, both automated and traditional, and verifies select operational functions.
  - Validates CDM Phases implementation rate and reported coverage
  - Provides feedback to DHS programs of gaps, deficiencies, and areas of concern for improvement.

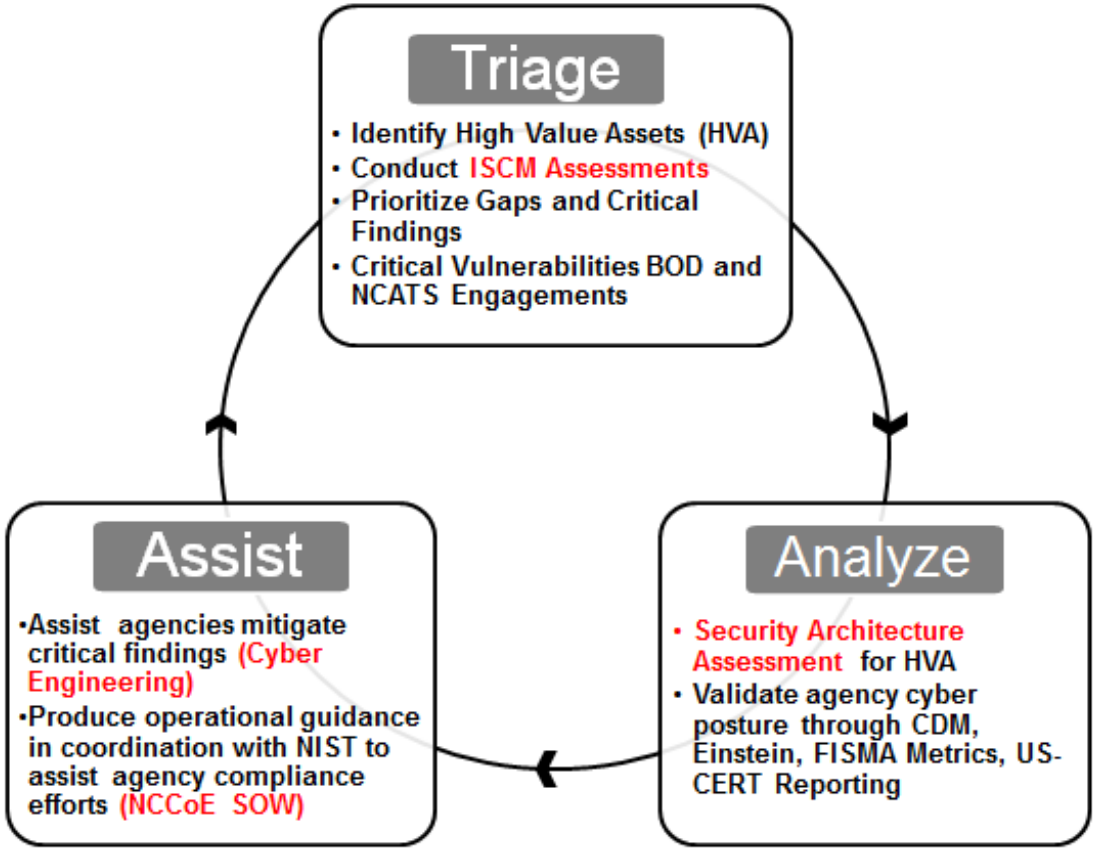
- **Staff Assistance and Verification –** Provides subject matter expertise to agencies in developing cybersecurity capabilities by verifying functional/operational procedures to meet program goals.
- **Binding Operational Directive Validation –** Develop evaluation criteria for select BOD's issued within the Cybersecurity Posture scope of interest and incorporate data points into the assessment methodology for scoring.

Homeland Security

CAB Security Assistance Approach

Strategy to deploy an adaptive and continuous engagement evaluation model based on continuously improving assessment methodologies

CAB Lifecycle Portfolio



Homeland Security

Security Assistance Value Proposition

Federal Audit Model

- Assessment Based
- Temporal Auditing
- Internally Facing
- Stagnant Criteria
- Insulated Information
- Prescriptive Reports

CAB Assistance Model

- Assistance Focused
- Continuous Engagement
- Externally Facing
- Adaptive Criteria
- Accessible Information
- Tailorable Reports

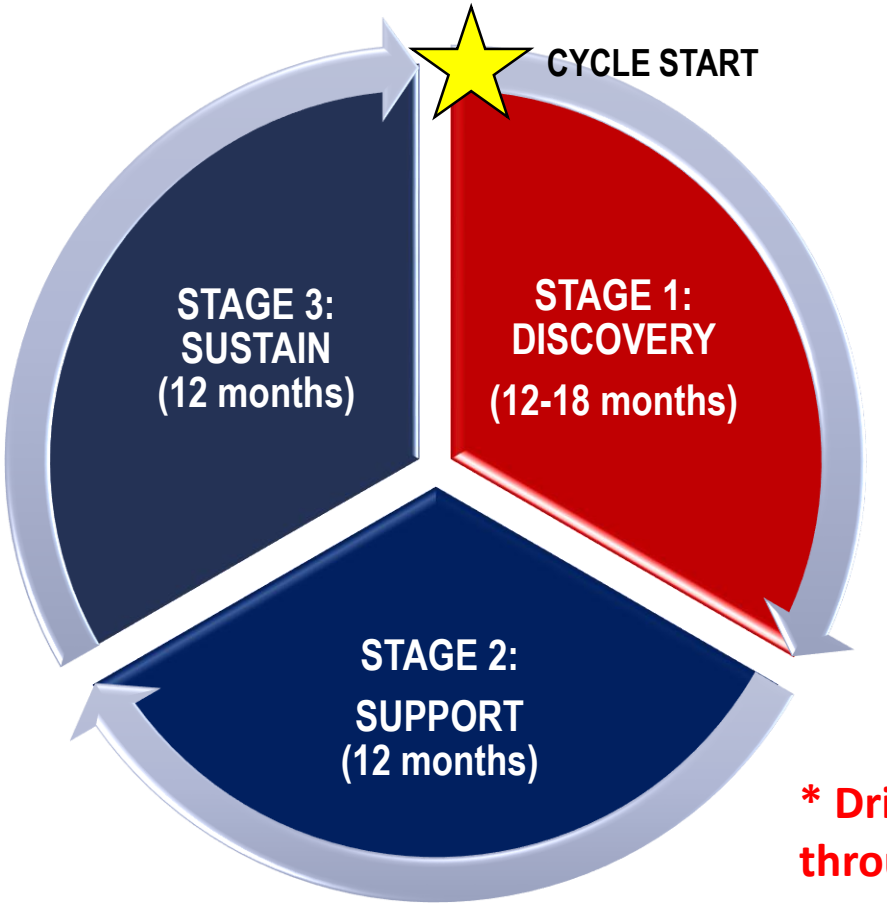
Homeland Security

OA Program Principles

- **Iterative and Adaptive Development (People, Process, Product)**
  - **3 year cycle of relevance for evaluation versions**
    - Issue updated assessment criteria based on lessons learned in previous cycle
    - Bake in mandatory improvements to evolve methodology and maintain relevancy
  - Iterative improvements throughout the cycle
  - Elicit input from agencies, lessons learned, and best practice
- **Verify and Validate Cybersecurity Programs**
  - Are we doing cybersecurity right?
  - Are we doing the right cybersecurity?
  - Are we providing and maintaining our programs properly?
- **Continuous engagement, continuous loopback**
  - Iterative improvements are adopted during one cycle for deployment in the next
  - Upstream and downstream feedback is incorporated
  - Build and maintain positive relationships and equities

Homeland Security

Example: the CAB Assistance Cycle



STAGE 1: DISCOVERY

- **Initiate assistance cycle**
- **Assessment #1**
  - Initial assessment baseline
  - Do they Implement the right cybersecurity?
- **Verify functional security (voluntary)**
  - Analysis and design of systems and programs. A limited view of "do they perform cybersecurity right?"
- **Develop initial Wellness Plan**
  - Plan of Action & Milestones
  - Engineering approach

STAGE 2: SUPPORT

- **Assessment #2**
  - Re-validation and gap analysis
  - Are they managing deficiencies?
- **Wellness support**
  - POA&M Update
  - Engineering Plan
- **Program Gap Analysis**
  - Define new capabilities based on program, operations, or industry

STAGE 3: SUSTAIN

- **Assessment #3**
  - Final Assessment
  - Are they planning for and adopting improvements?
- **Assess New Capabilities**
  - Non-scoring
  - Adopted next cycle
- **Closeout Wellness Plan**
  - POA&M Close out
  - Initiate Next Cycle Wellness Plan
- **Final Reporting for Cycle**

*** Drive improvements throughout the process!**

Homeland Security

Federal ISCM Evaluation

A modular evaluation of cybersecurity posture incorporating ISCM principles and other concerns

TASK 1 OBJECTIVES

- Measure the adoption and implementation of ISCM at agencies
- Quantify the impact of CDM in ISCM programs
- Determine the extent ISCM programs support risk management decisions
- Measure the readiness of agencies for ongoing authorization

Homeland Security

ISCM Evaluation

- Provides a foundation of cybersecurity goals which can then incorporate modular security domains for evaluation.
- Provide a **balanced scorecard** measuring ISCM implementation based on associated program perspectives to determine posture health
- Define automation gaps and assess compensating approach
- Validate and provide feedback to DHS programs
- All assessment activity will be based on and reference appropriate NIST standards and widely accepted best practices.
- *Assumption: Information Security Continuous Monitoring (ISCM) strategy represents a baseline technical foundation for prescribed cybersecurity implementation at this time*

Homeland Security

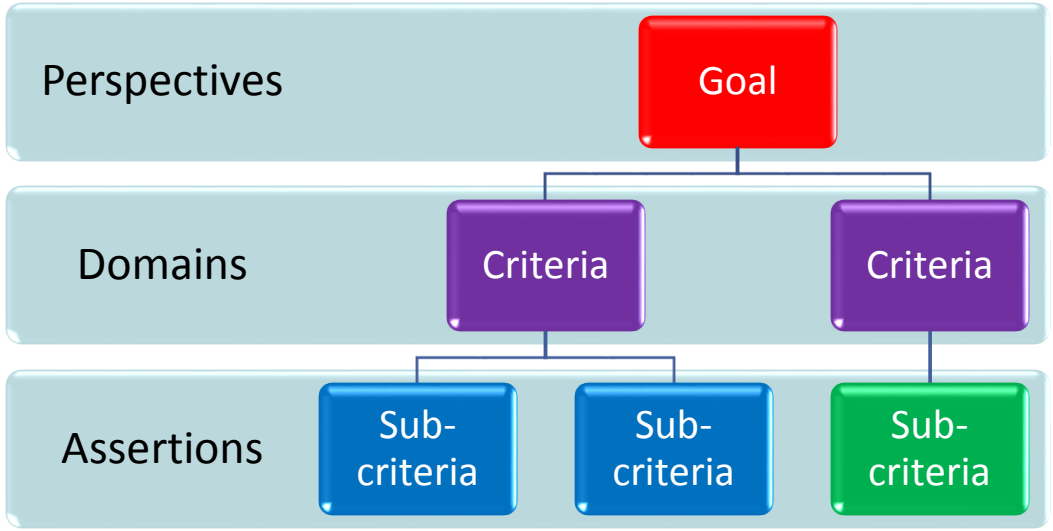
Guiding Principles

- **Focus on the basic principles of ISCM.**
  - Most agencies are just getting started.
- **Stay at a high level.**
  - Level should be more general than detailed approaches like CDM and NISTIR 8011.
  - Avoid being prescriptive.
- **Provide traceability to authoritative sources.**
- **Keep it simple and straightforward for both agencies and assessment teams.**
- **Be capable of adapting as agency programs mature.**
- **Provide value to agencies so that they desire this engagement regularly to measure their progress.**

Homeland Security

Evaluation Approach

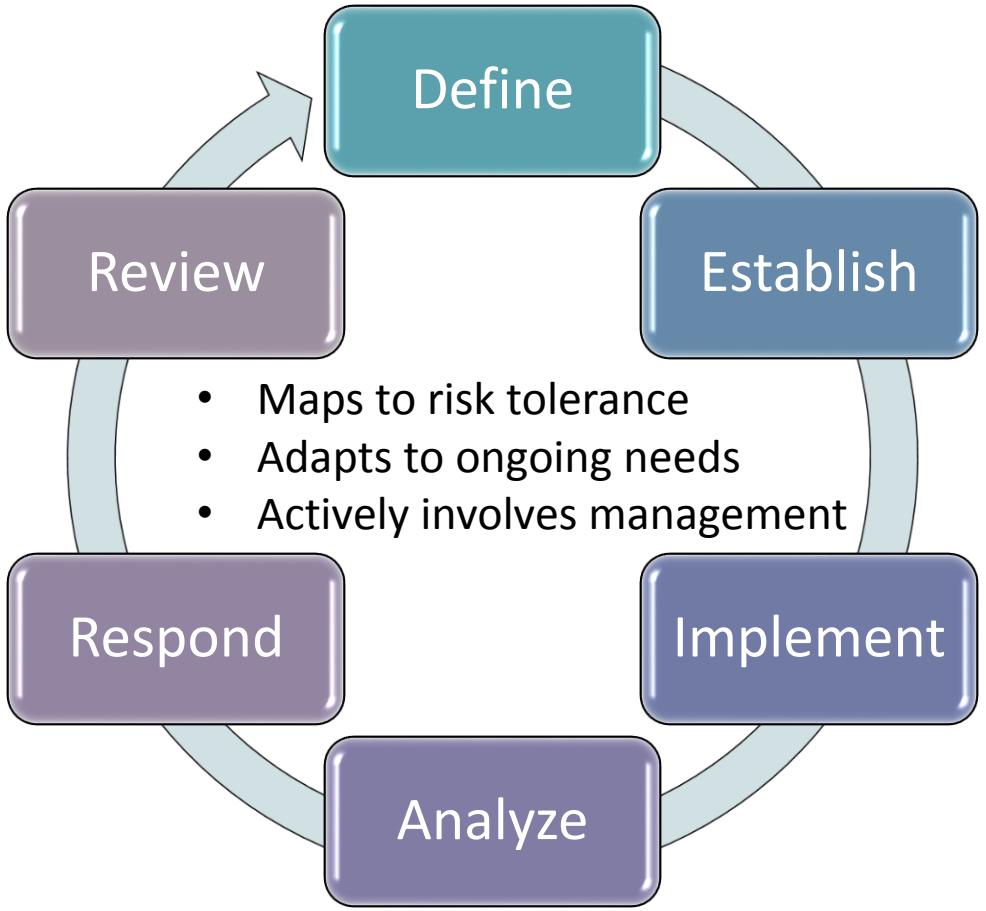
- **Workflow consists of 3 phases in collaboration with the environment owner:**
  - Preparation, Execution, and Delivery
- **Prepare baseline of environment**
- **Collect and review relevant data**
  - Documents: organizational policies and strategies, operational ISCM processes
  - Dynamic ISCM data: dashboards and reports
  - Human insight and interviews
- **Incorporate a sound process for analyzing ISCM based on assessment perspectives**
  - Develop relevant reports for external, internal, and temporal business requests



Homeland Security

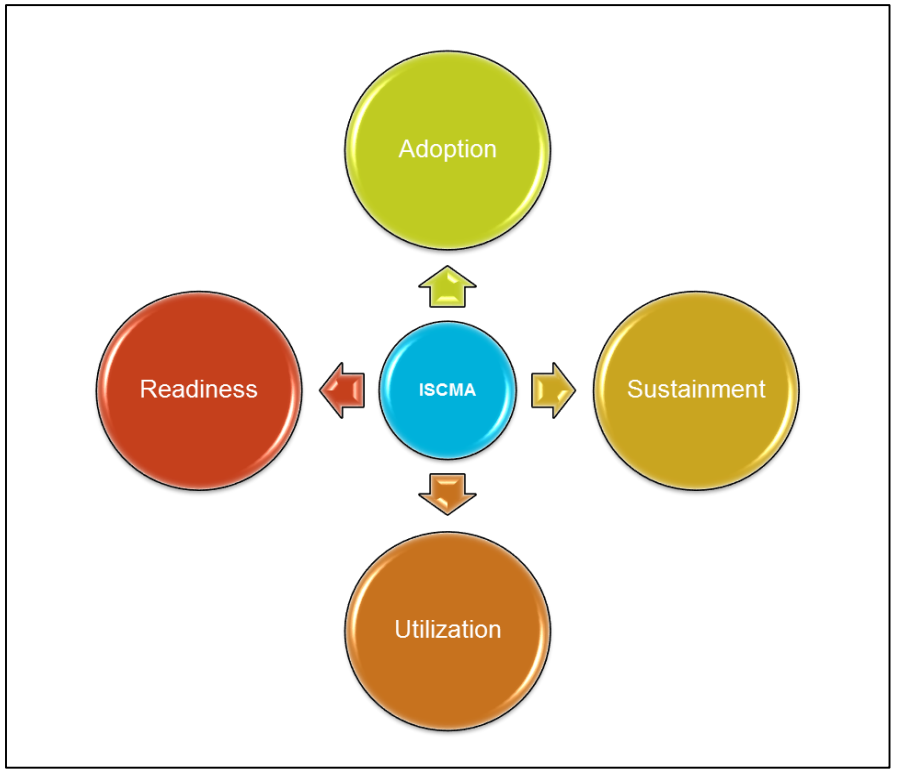
ISCM Process Steps

- **Define** the strategy
- **Establish** a program
- **Implement** the program
- **Analyze** and **Report** findings
- **Respond** to findings
- **Review** and **Update** the program and strategy



Proposed Assessment Perspectives

- **Adoption –** Measures the extent to which ISCM is defined and implemented
- **Utilization –** Measures the integration of ISCM program into the organizations technical and business processes
- **Readiness –** Measures the capability to use the ISCM program to inform the organization for Ongoing Authorization; as well as investments, mitigations, etc.
- **Sustainment –** Measures the degree to which the organization has established support structures to ensure long-term viability of ISCM program



Homeland Security

Breadth

- **The breadth of coverage is based on NIST SP 800-137, NIST SP 800-37, and OMB M-14-03, OMB A-130.**
- **The assessment structure can be viewed as a matrix**
  - Rows: The 6 process steps
  - Columns: The 4 assessment areas

	Adoption	Sustainment	Utilization	Readiness
Define				
Establish				
Implement				
Analyze/Report				
Respond				
Review/Update				

Homeland Security

Flexibility

- **The breadth is flexible.**
  - Begins with Define
  - Can stop after any step to accommodate less mature programs, e.g.,
    - Stop after Define (a “strategy” assessment)
    - Stop after Establish (a “design” assessment)
    - Stop after Implement (an “implementation” assessment)
    - Include all steps (a “full” ISCM assessment)
- **The scope of ISCMA version 1 is steps 1-3.**

Homeland Security

Assessment Scope

- **The assessment scope is a designated agency or possibly a major component of an agency.**
- **Assertions about "each mission/component":**
  - Are reviewed for each mission/component in the designated scope.
  - Must be true for all such missions/components, otherwise they are only partially true.
- **Assertions about "each information system":**
  - Are reviewed for each *high-value system* (at a minimum) in the designated scope.
  - Must be true for all reviewed systems, otherwise they are only partially true.

Assertion Development

- **Assertions are**
  - Statements to be validated by the assessment team
  - Associated with each cell of the matrix
  - At various levels of detail
- **Assertions are generally based directly on the statements related to continuous monitoring extracted from the authoritative sources.**
  - Some assertions were also expanded if this was deemed operationally necessary, e.g., data must be "current and complete" (SP 800-137 Section 2.6) was expanded, as shown in the examples [on the previous slide] of "timeliness."
  - Some assertions were reworded to mitigate ambiguity in the source documents, e.g., "Includes metrics that provide *meaningful* indications of security status"
- **Assertions are also annotated as being critical vs. non-critical, which impacts how they are scored.**

Homeland Security

Assertion Distribution

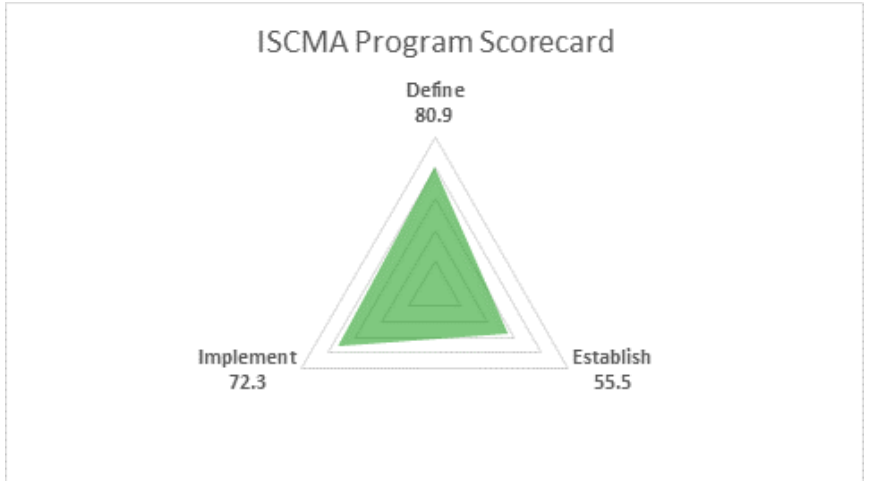
	Adoption	Sustainment	Utilization	Readiness	Total
Define	18	1	4	2	**25**
Establish	16	5	1	3	**25**
Implement	34	5	3	8	**50**
Total	**68**	**11**	**8**	**13**	**100**

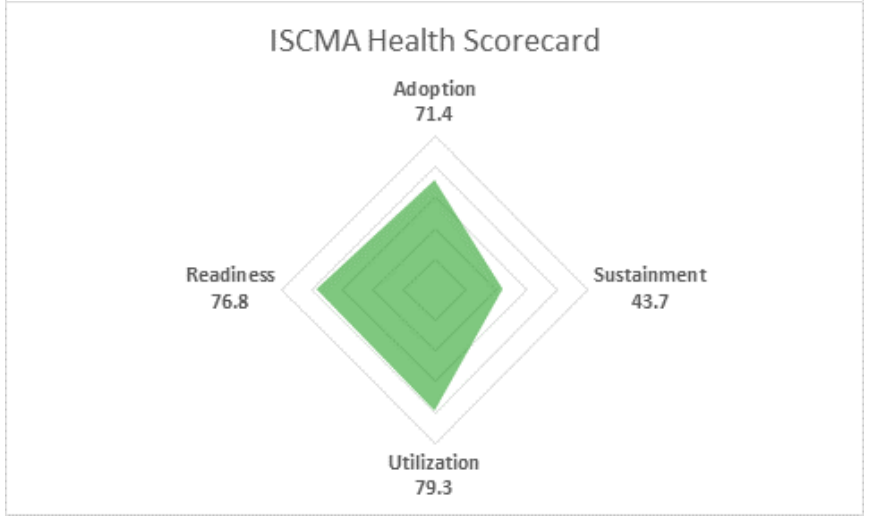
- **Sustainment, Utilization and Readiness will contain additional assertions when the remaining SP 800-137 steps are added.**
- **The contribution of a given assertion toward the total score is independent of the number of other assertions in its cell.**

Homeland Security

Cyber Posture Scorecard

- A balanced scorecard based on relevant performance perspectives
- Quantifies the health of ISCM strategy and implementation within agency
- Provides decision makers meaningful views of security posture
- Can be used to support maturity model determination





Homeland Security

Analytic Outcomes

- Where can efficiencies be found in the ISCM program?
- How is ISCM affecting risk decisions?
- What portion of ISCM program can be implemented via automation?
- What portion of the ISCM program is implemented via CDM?

Future Directions

- Implement frequent process improvements, especially early in deployment.
- Add Process Steps for Analyze/Report, Respond, and Review/Update.
- Add privacy assertions, as ISCM and Privacy Continuous Monitoring programs are often combined into a single program.
- Explore other scoring techniques.
- Explore integration with existing assessments of maturity level.
- Explore integration with the CyberSecurity Framework.
- Explore ways of addressing outcomes (vs. outputs)

Homeland Security

Thank you!

Please contact Chad Baer (DHS) with any further questions!