



ISOAG Meeting August 30, 2017

Welcome to CESC



Welcome and Opening Remarks

Michael Watson

August 30, 2017



ISOAG August 30, 2017 Agenda

- | | |
|---|--|
| I. Welcome & Opening Remarks | Mike Watson, VITA |
| II. Risk Assessment process definition and system assessment | Eddie McAndrew, Impact Makers & Barry Davis, VDSS |
| III. Changes to SSAE-16 and SOC standards | Benamin A. Sady, Dixon Hughes Goodman |
| IV. The Virginia Information Sharing and Analysis Organization (VA-ISAO) | Catherine Petrozzino, MITRE Mid-Atlantic Cyber Center |
| V. Upcoming Events | Mike Watson, VITA |
| VI. Partnership Update | Northrop Grumman |

ISO Services

Funding & Delivery

a VDSS Experience



VIRGINIA DEPARTMENT OF
SOCIAL SERVICES

!impactmakers

1707 Summit Avenue, Suite 201
Richmond, VA 23230

Barry Davis, CISSP

DSS Chief Information Security Officer

Eddie McAndrew, CISSP

Impact Makers GRC Lead Consultant

ISOAG 8/30/2017



Agenda

- DSS Background
- Requirements development
- Procurement process
- Impact Makers approach
- Project Components
- Next Steps for DSS



DSS Background

- 46 sensitive systems
- BIA with 269 business functions
- Mature CP
- Last SEC501 RA in 2007
- Lost institutional knowledge of performing RAs
- DPB Funding



Requirements Development

- Needs
 - 46 Risk Assessments (RAs)
 - Training for staff who haven't done RAs
 - Documented process
 - CP/BIA assessment
- Timing (already Q2 of FY16)
- Target 22 RA by end of FY16
- Business Impact Analysis (BIA) review (are we on track?)



Procurement Process

- Statement of Requirements (SOR) development
 - 1st step in procurement process
 - Defines key elements of requirement
 - Starts the discussion
- Estimates and SOR review
 - Known partners?
 - CAI has contact info for providers
- Engaging CAI Managed Service Provider (MSP)
- SOW back from vendor & negotiations
 - Value added discussion!
 - CP Table Top became RA Knowledge Transfer
- Signed SOW (post negotiation & mods)



Making it Happen

- Broadcast announcement to system owners, Agency Head – key stakeholders
- Project Kickoff
- Designated DSS POC for scheduling
- Follow-up with system owners
- Risk Assessment Interviews—
 - Management
 - Technical



Impact Makers Approach

- Strategize with DSS
 - Long term goals
 - Short-term needs
 - Focus on achieving while minimizing cost
- Integrate Best Practice with COV Compliance Requirements
 - Compliance requirements
 - Security program development
- Work with DSS to ensure SOW meets the need



The Project– BIA Assessment

- Mature Continuity Plan (CP)
 - Key stakeholders engaged in process
 - Fundamental processes in place
- Document review & Interviews
 - Stakeholder observations
 - Opportunities for improvement
- Opportunities for Security Program Integration
 - Data classification
 - Overarching policy considerations

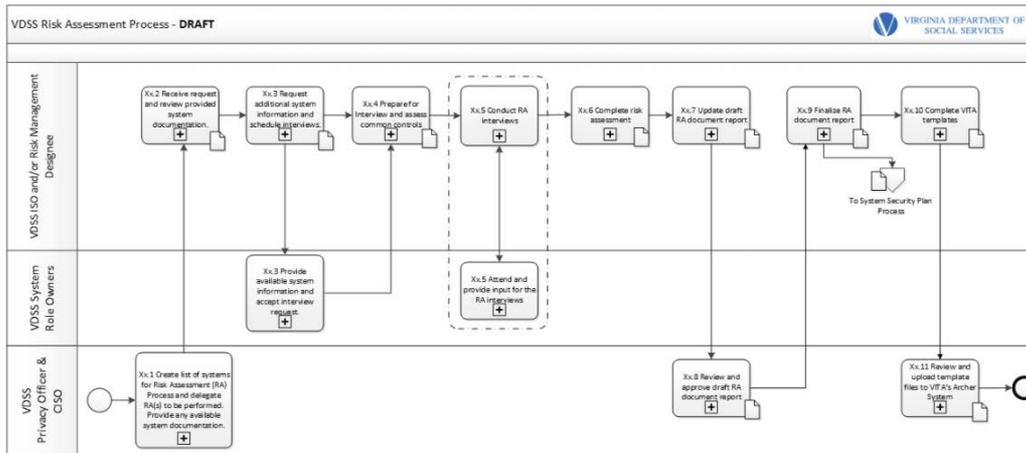


The Project– Risk Assessment Process Development

- Assess current environment – no currently defined process
- Leverage SEC 501 and 520 Frameworks
 - Fundamental underpinning of process
 - Provides compliance while building program
- Leverage Industry Best Practices
 - NIST 800-37
 - Structured approach to provide consistency
 - Full transparency
- Collaborate with key stakeholders in process design
- Refining through use
 - Iteration is key
 - Engagement with DSS RA team



The Project– Risk Assessment Process Development



VIRGINIA DEPARTMENT OF SOCIAL SERVICES	Process Name	Risk Assessment (RA) Process Narrative
Process Number	VDSS-XXX	Process Owner Barry Davis VDSS Privacy Officer & Chief Information Security Officer, Information Security and Risk Management Office
Revised By	Impact Makers	Revision Date 02/XX/2017
Version Number	V1.0	Effective Date XX/XX/2017
Previous Version Number	N/A	Previous Version Date N/A
Approved By		Approval Date

Process Description	<p>The Risk Assessment (RA) process delineates the steps VDSS will take for each IT system classified as sensitive to:</p> <ul style="list-style-type: none"> Identify potential threats to an IT system and the environment in which it operates; Determine the likelihood that threats will materialize; Identify and evaluate vulnerabilities; and Determine the loss.
Process Triggers	<ul style="list-style-type: none"> Time Elapsed (3 Years) for full process Annual review and update in interim years New system is added to the environment Significant change occurs in an existing system
Process Participants	<ul style="list-style-type: none"> VDSS Privacy Officer & Chief Information Security Officer VDSS designated ISO and/or risk management staff member(s) System Role Owners <ul style="list-style-type: none"> System Owner Data Owner(s) System Administrator(s) Application Administrator(s) Data Custodian(s)
Process Inputs	<ul style="list-style-type: none"> Current VDSS Risk Assessment Plan Updated Data and System Classification Report



Project Elements – Risk Assessment Execution

- Identify the DSS RA team and relevant stakeholders
- Identify and leverage common control families
- Obtain available system documentation up-front
- Conduct interviews with technical subject matter experts
- Obtain buy in on draft RA reports
- Integrated assessment approach to facilitate prioritized risk treatment plans/mitigation strategies



RA Knowledge Transfer

- Getting the job done while transferring knowledge
 - Meet the requirements
 - Engagement of the DSS team in the creation of the process
- Refining the process as a part of completing risk assessments
 - Iteration is the key to both developing the process *and* transferring the knowledge
 - Buy-in is central to organizational change management (OCM)
- Creating the capability within DSS
 - Central to the Impact Makers Approach



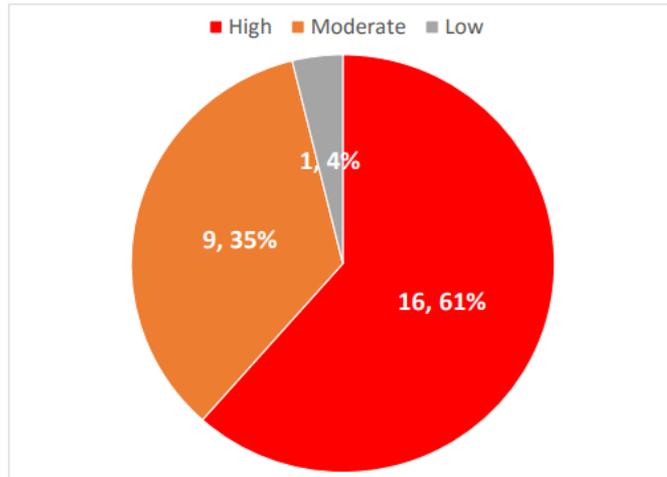
The Project - Metrics

- Insights for focus – severity vs bang for the buck!
 - Close most significant exposures
 - Prioritize remaining based on most cost effective approach
- Trend analysis over time
 - Use metrics to understand organizational behavior
 - Structure approach to mitigate risks accordingly
- Demonstrating progress
 - Key to executive involvement
 - Provides a means to demonstrate resource requirements



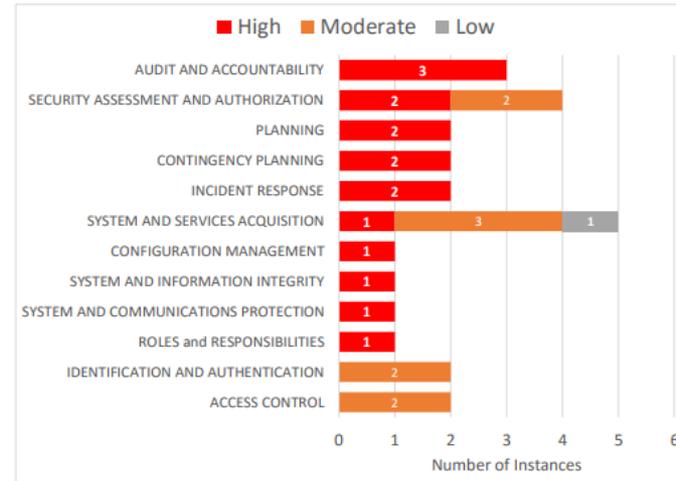
The Project – Metrics Examples

**Risk Ratings Distribution –
OpenLDAP**



This graph highlights how many total risks were identified, as well as their overall criticality.

**Risk Ratings by Control Family –
OpenLDAP**



This graph highlights how many risks were identified by control family, as well as their overall criticality.



DSS Next Steps

- Complete remaining RAs (23 remaining)
- Integrate adopted recommendations for BIA/CP into execution
- Execute RA remediation strategies
- Continues to improve security program



Questions & Answers



Thank You!



Artifact Slide

- Sample SOR



Sample RA
Statement of Requirement

- RA Procedure



RA Process
Narrative

- RA Process Map



VDSS RA Process
Map





DHG

DIXON HUGHES GOODMAN LLP

SOC Framework Updates

August 2017



The Virginia Information Sharing and Analysis Organization (VA-ISAO)

Cathy Petrozzino
Project Leader
August 2017

VA-ISA0 Agenda

- **What is the VA-ISA0**
- **ISA0 Value Challenge**
- **VA-ISA0 Innovation and Essentials**
- **Timeline**
- **What is the Ask?**

ISAO/ISAC: Organizations created to gather, analyze, disseminate cyber threat information



VA-ISA0



- On April 20, 2015 Gov. McAuliffe announced nation's first state-level ISA0
 - Regional
 - Supports public and private cross-sector organizations

- Secretary Jackson: “leverage our existing and future information sharing efforts”
- Seed funding allocated for FY17 and FY18
- The MITRE Corporation tasked with standing up the VA-ISA0



Why MITRE?

Independent
Trusted

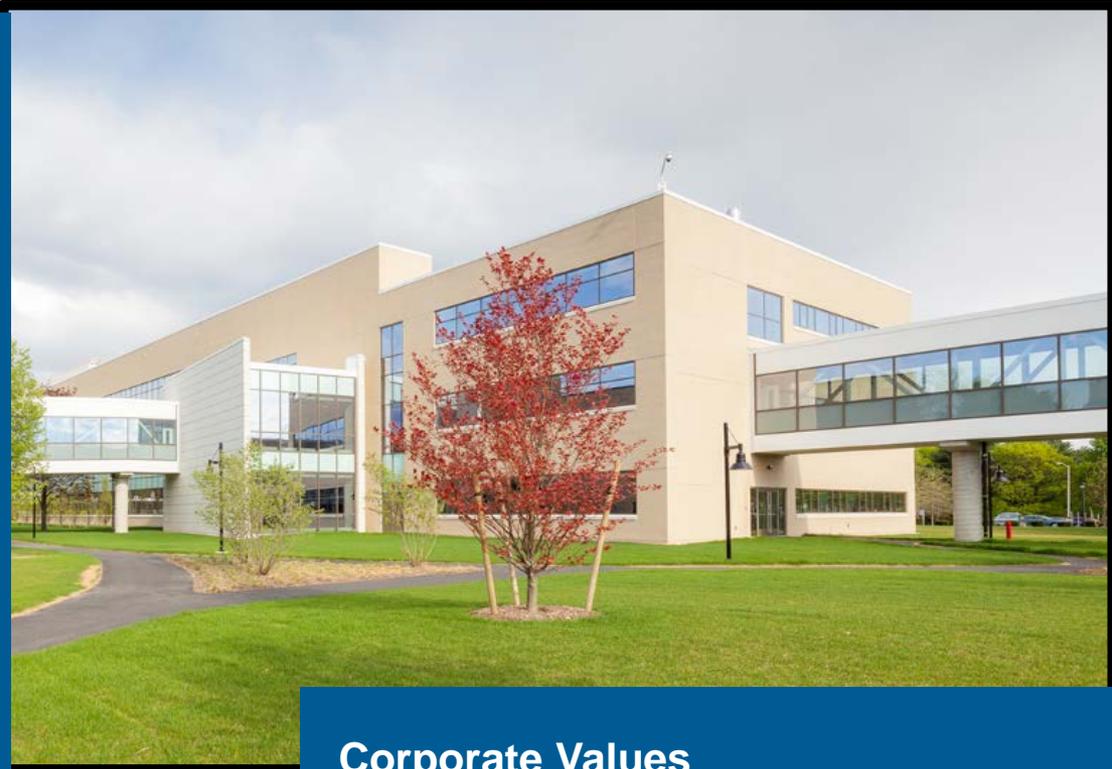
over
1,000
people

experience

tech center

innovation
program

focus on
partnerships



Corporate Values

- Serve the public interest
- Culture of sharing
- Strengthen the nation's cyber defenses
- Improve our cyber defenses

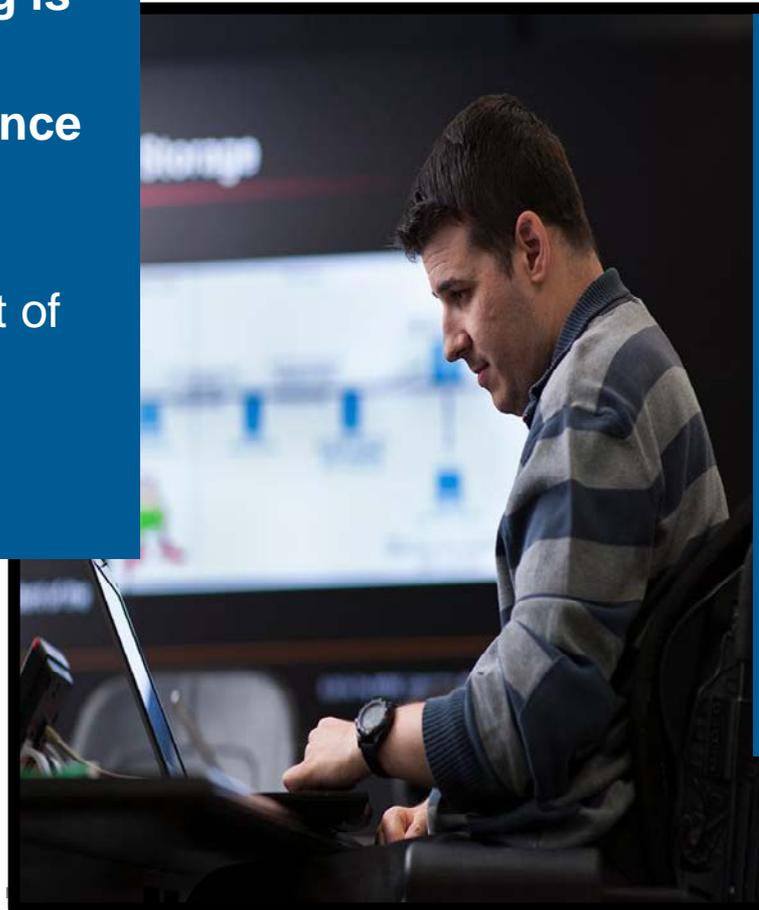
Realizing the Cyber Sharing Value

Survey of 300+ ‘threat experts’

- Cost of hacking is decreasing
- Threat intelligence sharing is best defense
 - Number 1 out of 21 defensive options

Sharing Reality

- Only 33% of organizations say they are satisfied with sharing efforts ⁽³⁾
- 27% of respondents believe their organizations are “very effective” in utilizing threat data ⁽⁴⁾



Deeper Dive into the ISAO Value Challenge

- **Uneven value proposition across membership**
- **Frustration with participation imbalance**
 - Small number of organizations ‘producing’ threat information
- **Technology heavy sharing**
 - “I don’t even know where to begin” (quote from a have-not)
- **Lack of trust due to different cyber abilities**
 - Separate rogue sharing groups
- **Exacerbated by lack of cyber security resources**
- **Exacerbated by lack of ISAO resources**
 - Membership and sustainment always a challenge
 - Since Gov McAuliffe’s announcement, five other states ‘ISAOs’

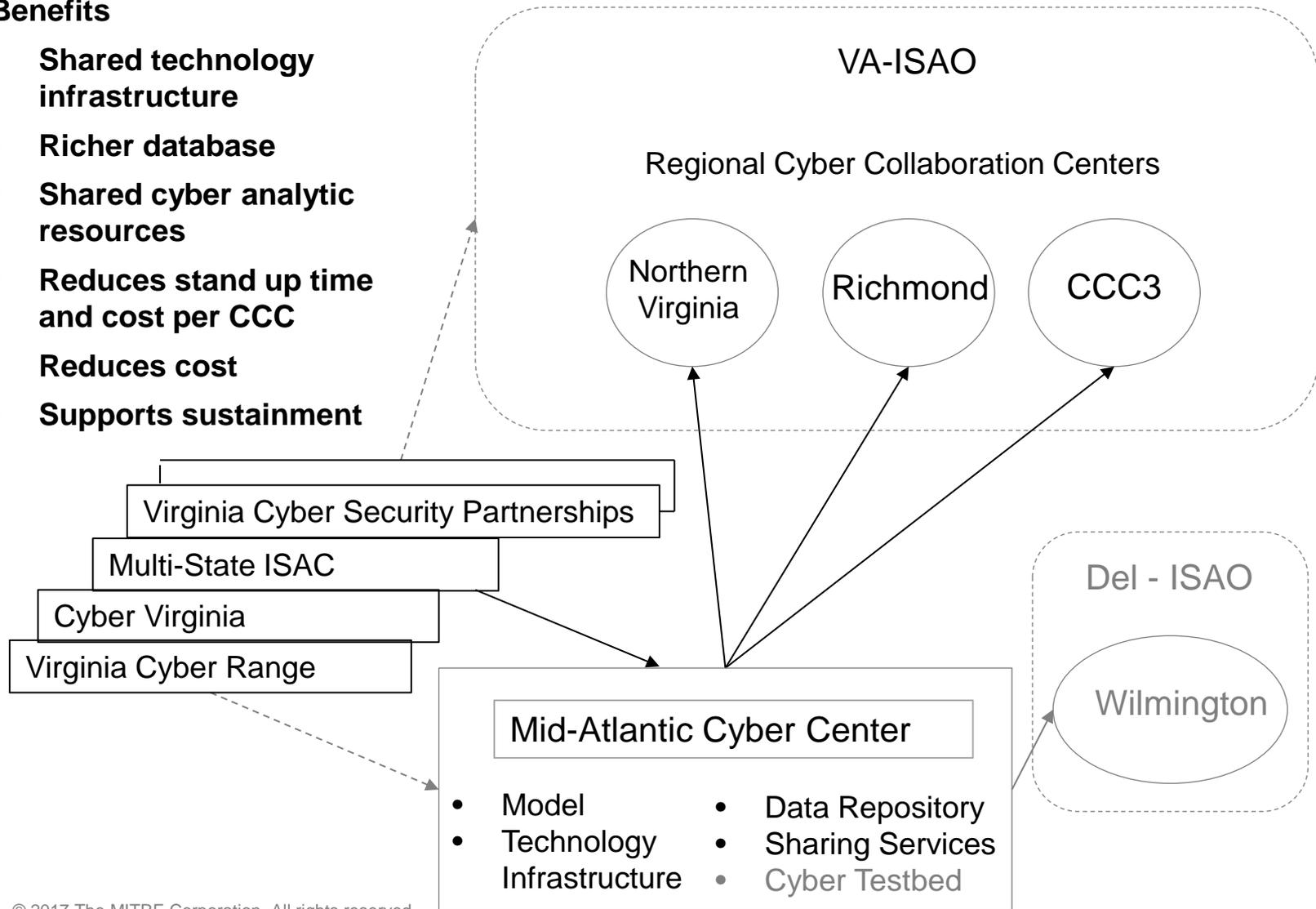
VA-ISA0 Innovation

- **Shared resources model through the Mid-Atlantic Cyber Center (MACC)**
- **Welcomes organizations from other states**
- **Personalization**
- **Cyber diversification**
- **Recognizes effective cyber requires more than technology**
- **Recognizes that cyber programs should vary with organization/threat**

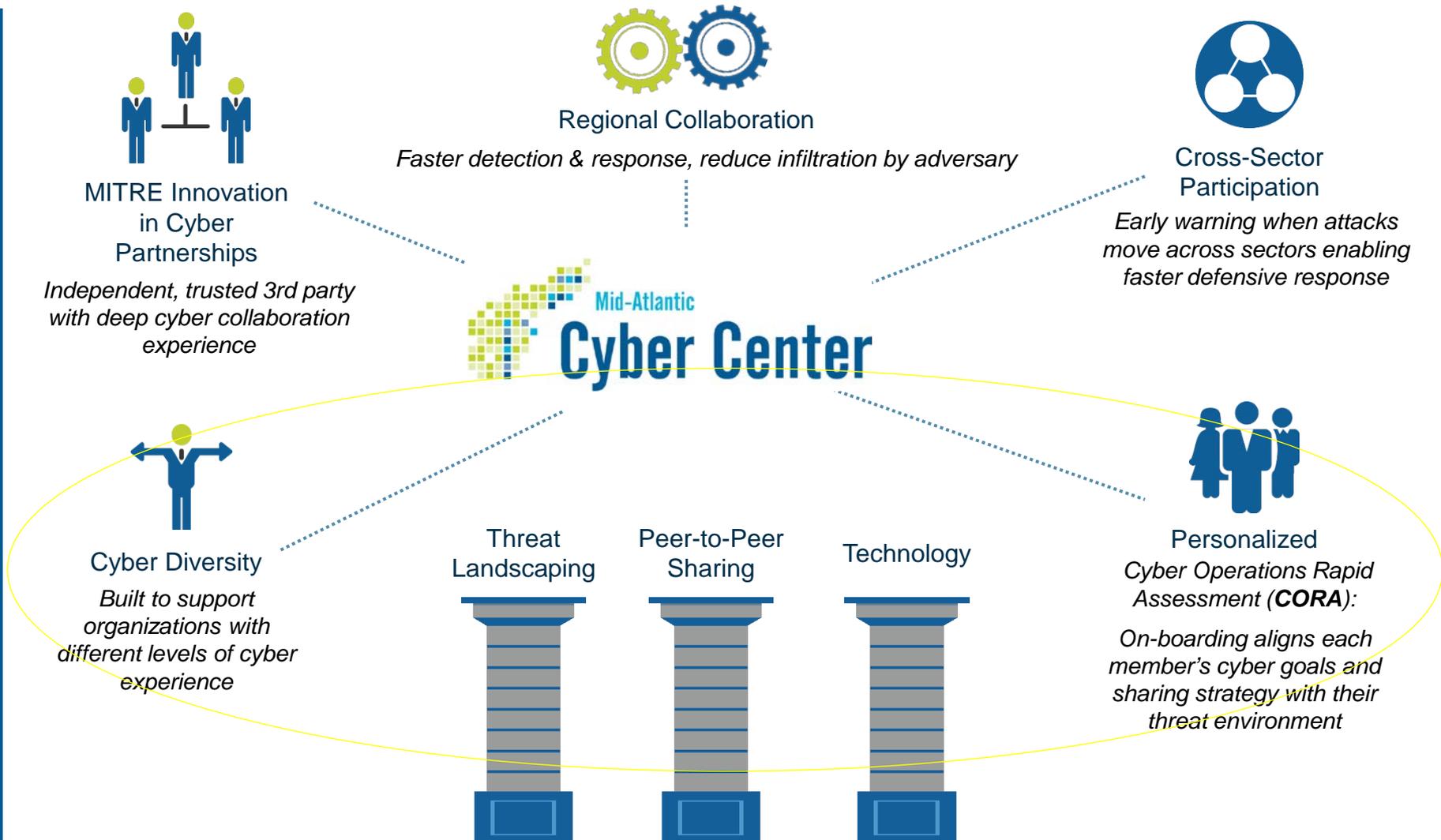
VA-ISAO/MACC Ecosystem

Benefits

- Shared technology infrastructure
- Richer database
- Shared cyber analytic resources
- Reduces stand up time and cost per CCC
- Reduces cost
- Supports sustainment



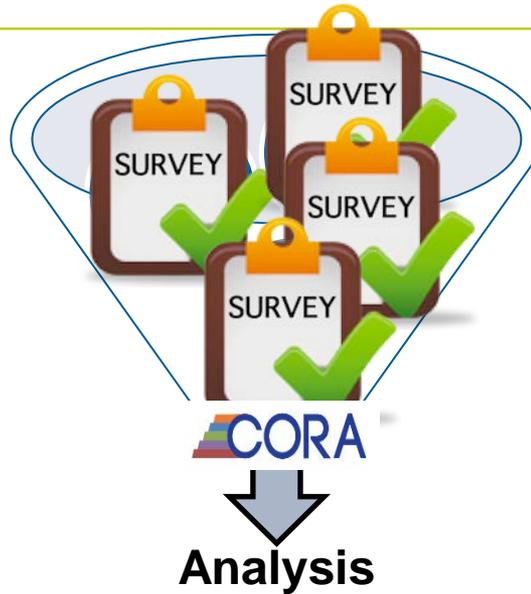
VA-ISAQ/MACC Essentials



CORA Survey Content Areas



Outputs from Onboarding Survey



Participants' Cyber Stats

Personalized Threat Profiles

Relevant Topic Areas

Collaboration Groups

Maturing a Risk-Based Cybersecurity Program



		FOUNDATIONAL	DEVELOPING	ESTABLISHED	<i>Value to Organization</i>
AWARENESS & TRAINING	Leadership, defender and employee understanding of organization's cyber risk:	MINIMAL	PARTIAL	THOROUGH	RISK-BASED FOCUS ON RELEVANT THREATS
EXTERNAL ENGAGEMENT	External threat information sources regularly utilized and shared (ISAC/ISAO, govt, open source, commercial):	NONE	PASSIVE	ACTIVE	COMMUNITY-WIDE VISIBILITY & HERD IMMUNITY
INTERNAL PROCESSES	Staffed and resourced cyber program, policies, concept of operations:	MINIMAL	PARTIAL	THOROUGH	ABILITY TO RESPOND TO THREATS
TOOLS & DATA COLLECTION	Defensive technologies/controls and security log, sensor, event data collection:	MINIMAL	COMPLIANCE-DRIVEN	THREAT-DRIVEN	INTERNAL VISIBILITY & PROTECTION
TRACKING & ANALYTICS	Indicator and incident tracking, management, and analysis:	AD HOC	LOOSELY STRUCTURED	STRUCTURED	SENSEMAKING, DECISION MAKING ABOUT THREATS

The MACC Soft Launch



**Limited pilot to
validate enhanced
value proposition**

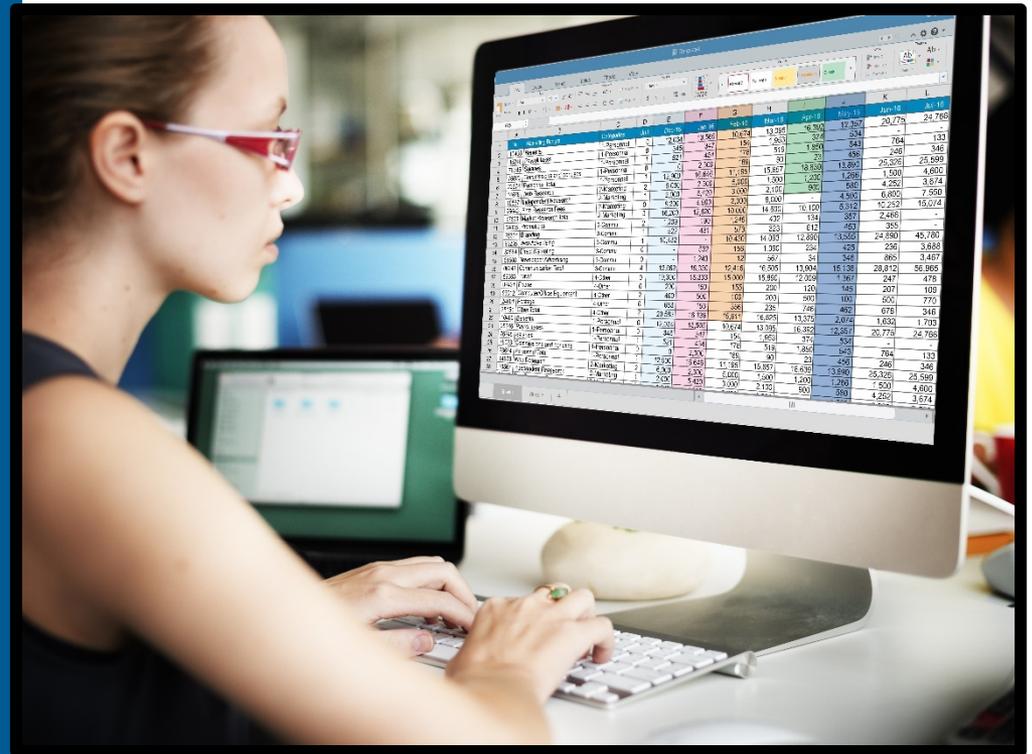
**Cross-sector,
diverse group**

**3rd meeting: Sept
12: Evolving a
Cyber Program**

**Scheduled end: Fall
FY17**

VA-ISAO CCCs

- Northern VA: Sept/Oct CY17
- Richmond: early CY 18
- Relies on private sector financial support
- Seeking other grants
- MACC 'stand up' phase is 2 years, followed by a transition



Our Ask...

- Feedback on your cybersecurity needs
- Participation
- Talk to your (C)ISO friends
- Suggestions



▪ **Cathy Petrozzino**

— cmp@mitre.org

▪ maccisao@mitre.org

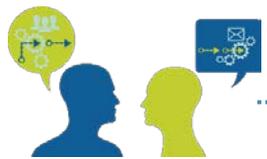
References

- 1) DHS Frequently Asked Questions about Information Sharing and Analysis Organizations
- 2) Flipping the Economics of Attacks, January 2016
- 3) 2015 Ponemon Second Annual Study on Exchanging Cyber Threat Intelligence: There Has to Be a Better Way , November 2015
- 4) The Value of Threat Intelligence: A Study of North America and United Kingdom Companies , July 2016

Back-Up

VA-ISAO Vision – Elevated, More Even Value Proposition

A Next Generation, Regional, Cross-sector Cyber Collaboration Center that:



Incorporates best practices of successful collaborations and trust sharing



Implements new strategies to enhance the value of collaboration



Adapts to the full range of the members' cyber abilities



Is sized and customized to enable true peer-to-peer sharing



Uses advanced tools, technologies and analytics



Leverages MITRE's and the collective members' experiences

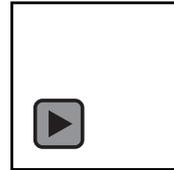


Is member driven with MITRE support



Follows direction and priorities set by Founding members

Today's Cyber Challenge



[Planet Money, Episode 610, The Prisoners Solution](#), 2015, updated 2017



Virginia Information Technologies Agency

Upcoming Events





Future ISOAG

NO SEPTEMBER MEETING

October meeting changed to 2nd Wednesday of the month

October 11th Meeting Mandatory

Speakers:

ISOAG meets the 1st Wednesday of each month in 2017



(ISC) 2 Meeting

(ISC)2 Richmond Metro Chapter meeting will be held on August 31st between 6 pm and 8 pm at John Tyler Community College Midlothian Campus. 800 Charter Colony Parkway, Midlothian VA 23114



IS Orientation

When: Thursday, Sept 21, 2017

Time: 1:00 –3:00 pm

Where: CESC , Room 1221

Presenter: Ed Miller

Register here:

<http://vita2.virginia.gov/registration/Session.cfm?MeetingID=10>



Announcement: VASCAN Conference 2017



IOT: The S Stands for Security

Date: September 28-29

Location: Virginia Tech, Blacksburg VA

Keynote Speaker:

Doug Wylie

Director Industrials &

Infrastructure Portfolio

SANS Institute

To Register: <http://www.cpe.vt.edu/vascan/>



SAVE THE DATE

"2018 COVA Information Security Conference: "Expanding Security Knowledge"

April 12 & 13

Location: Altria Theater

ADJOURN

THANK YOU FOR ATTENDING

