WELCOME TO THE March 6, 2024 ISOAG MEETING

VIRGINIA IT AGENCY

Information Security Officer's Advisory Group

March 6, 2024

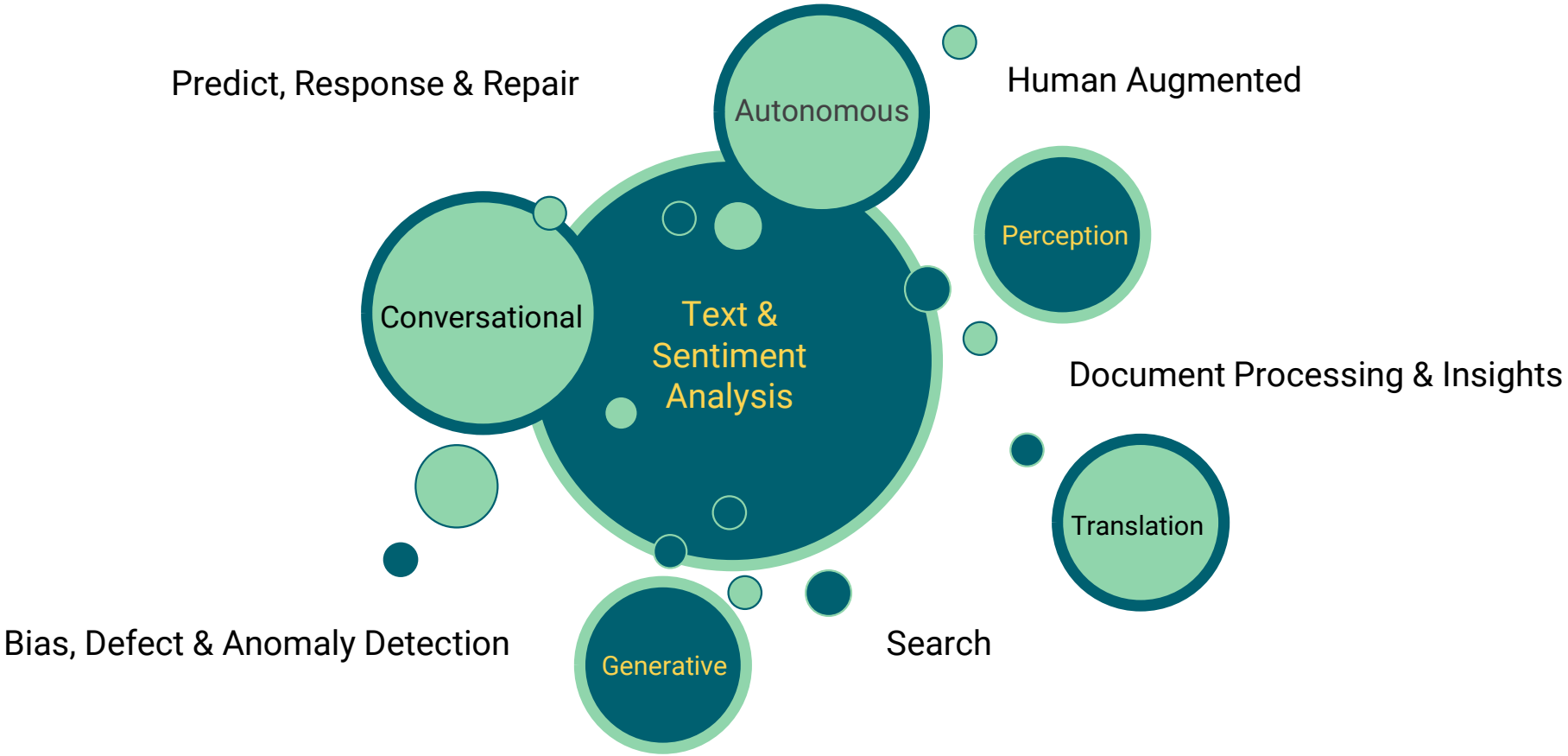
VIRGINIA IT AGENCY

Agenda	Presenter
Welcome/Opening Remarks	Erica Bland/ VITA
AI Registry	Stephen Smith/VITA
Governance and Compliance Updates	Amy Braden/ VITA
Outreach and Education, Looking Ahead	Kendra Burgess/ VITA
Highlights from the 2023 TTX	Zachary D Wilton/SAIC
Upcoming Events	Erica Bland/ VITA
Adjourn	

ARTIFICIAL INTELLIGENCE (AI)

Unpacking EO 30 Policy & Standard

WE WANT TO USE AI



AI Policy & Standards

Utilization of AI by COV Policy Standard

- **Ethical Use** — AI solutions must be resilient, accountable, and explainable; AI models must be documented; AI outcomes must be validated for bias
- **Business Cases** — AI must be the optimal choice for a stated result and produce positive outcomes for COV citizens
- **Mandatory Approval** — each use of an AI solution must be recorded in an AI central registry and reviewed for approval by VITA and the secretariat
- **Mandatory Disclaimers** — public disclosure when AI is used to produce any decision or output, including how decisions were produced
- **Risk Mitigation** — AI vendor health assessment as part of procurement
- **Protect Citizen Data** — notification and required consent when using citizen data, and the security of sensitive and protected information

Enterprise Architecture AI Standard

- **Safety** — AI systems must be employed in such a way that they cause no harm to people, businesses, or the environment
- **Privacy** — data collected, leveraged, or trained in an AI System must be untraceable back to an individual
- **Transparency** — use of AI solutions in COV systems must be clear as to their use, extent, and value
- **Accountability** — risks associated with COV decisions must always remain with humans to avoid potential bias and discrimination by AI systems
- **Sustainability** — building and fostering skills that will support COV into the future and not lead to automation complacency or de-skilling

AI Registry overview

- Agency provides data: purpose, technology used, sensitivity, model algorithm, data sets used, & operation method

Registration

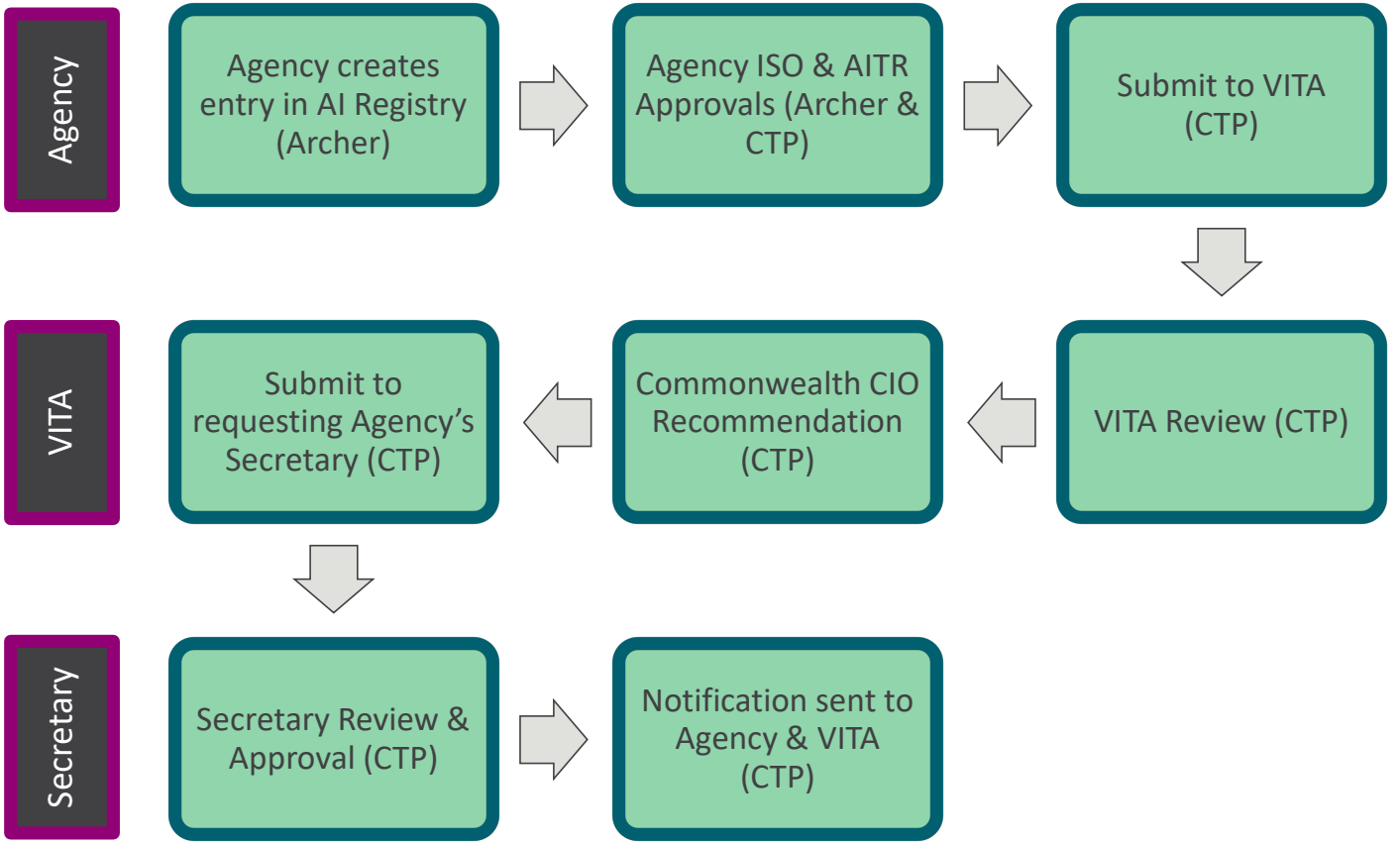
- Agency review/approval by ISO, AITR & AH
- VITA/CIO review & recommendation
- Final review & approval by responsible Secretary or designee

Approval

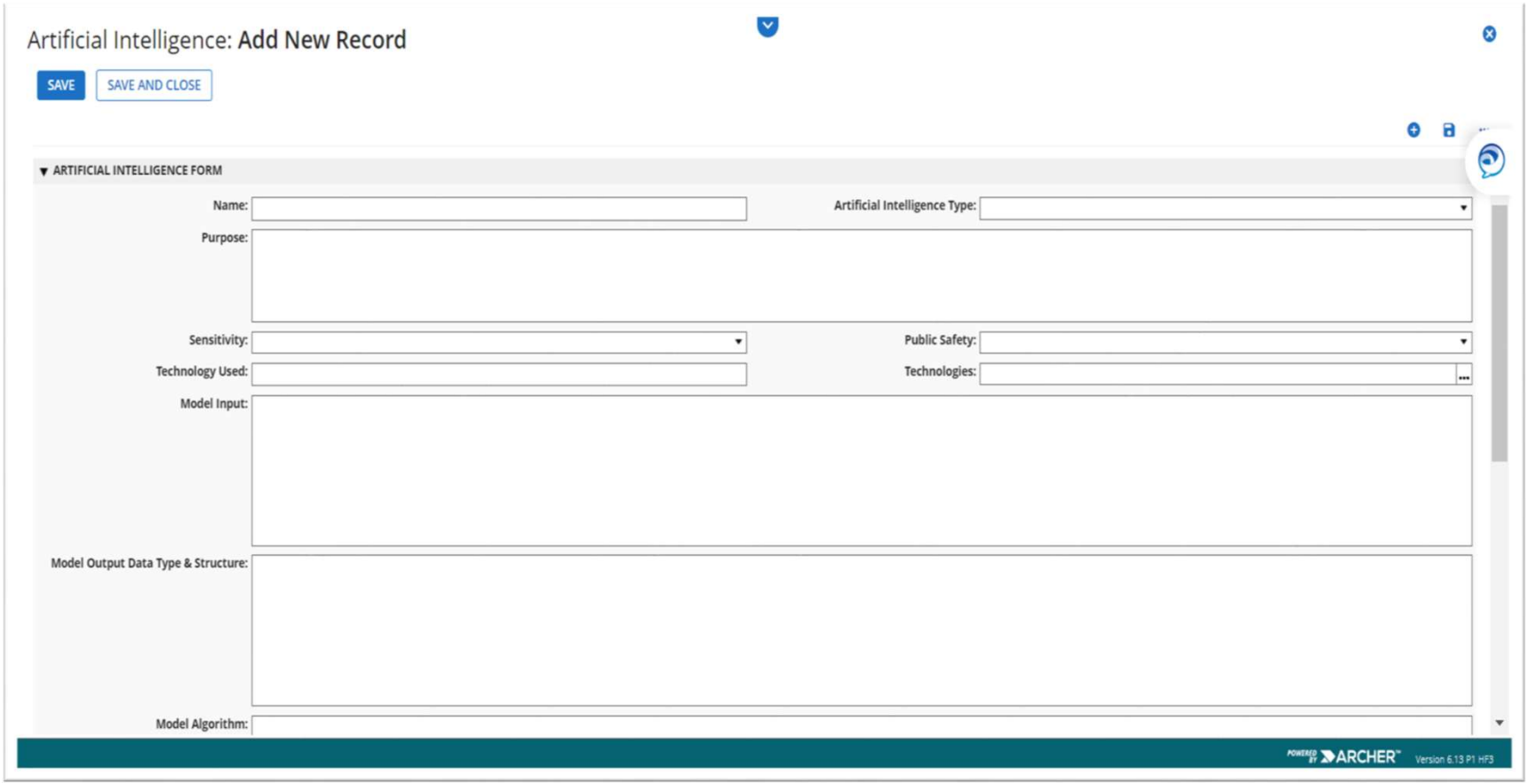
- Annually, for continued use (ISO via Archer)

Recertification

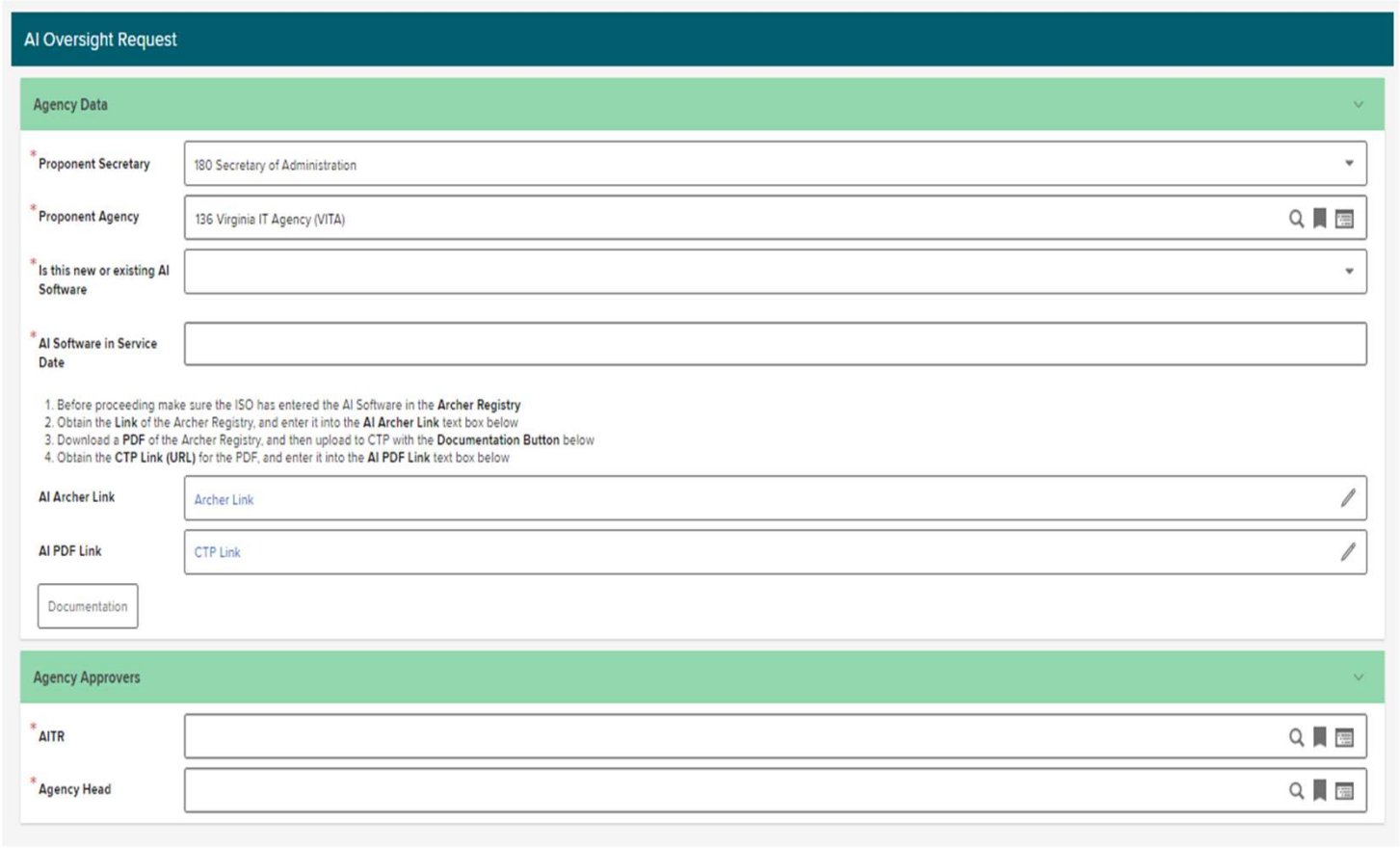
AI Registration & approval workflow



AI Registry walkthrough — Use case, technology & risks - Archer



AI Registry walkthrough - application to obtain approvals - CTP



AI Technology roadmap

Resources

- VITA webpage on AI: https://www.vita.virginia.gov/artificial-intelligence/
- We are here to help, and we welcome the opportunity to work with you! Contact your assigned EA architect or ITIMD analyst for questions and assistance!
- https://www.vita.virginia.gov/technology-services/cams-other-contacts/

Thank you!

March 6, 2024

VIRGINIA IT AGENCY

Governance and Compliance Updates

Amy Braden

Director, Security Governance

Amy Braden, Governance Director, CSRM

Key points

- Agency Grades
- Archer Clean-up
- Agency Review of ITSP SOC reports

Archer Data Clean-up Developments

March 6, 2024

Looking to What is on the Horizon

VIRGINIA IT AGENCY

CSRM Outreach and Communications

Kendra Burgess, VITA

Information Security Education and Relationship Management Specialist

March 6, 2024

COV Tabletop Exercise 2023 Summary

Zachary D. Wilton
SAIC MSI Security Incident Response

SAIC
Redefining Ingenuity

Agenda

MSI SIRT Information
2023 Event Overview
Event Feedback
- Scenario Example
- Strengths
- Areas for improvement

Additional SIRT Information

MSI Security Incident Response Team

Team Manager: Stephone Dixon

Shared Email: msi-security-operations@saic.com

Working hours: 7AM-7PM Active Monitoring with a 24x7 On-Call shared weekly

Our Role in the COV:

- Manage the Security Incident Response process
- Coordinate Service Tower communications, resources, and escalations for security incidents
- Ensure proper documentation of the Security IR process (primarily via Archer INC tickets)
- Manage and plan the annual COV Tabletop Exercise with the ATOS MSS and VITA CSRM
- Update the COV Incident Response Plans, as well as other Security IR related documentation

2023 Event Overview

Where/When:

- Exercise was Thursday, Oct 26th, 2023, from 8:00AM-2:00PM EST
- Hotwash was Friday, Oct 27th, 2023, from 11:00AM-12:00PM EST
- Total Event: 7 hours (Including a 15 min break and a 30 min break)
- All Virtual via Zoom Meeting

Who:

- Hosted by MSI SIRT team, ATOS Security, and VITA CSRM
- Participants included:
  - 8 Service Tower Suppliers (Full STS participation!)
  - 17 Executive Agencies

What:

- 16 Incident Response Scenarios submitted via Email
- Multiple Discussion questions shared/discussed on the Zoom presentation
- After-Action Review, included live event feedback and overall Security IR questions via Zoom

2023 Event Overview

Objectives:

1. Ensure essential job functions, roles, and technologies are operational, and processes are followed during a large-scale security incident.

2. Identify any gaps in response execution of procedures that do not meet or exceed expectations relative to continuity of operations and service level agreements.

3. Validate currency of procedures using scenarios representing real threats. Evaluate preparedness, communications, responsiveness, and processes for the presented scenarios involving the Service Tower Supplier or Agency.

4. Educate and train Suppliers to participate and work together to identify gaps in communication and processes to address challenges posed during a security incident in the decision-making processes and at the local, regional, and statewide level.

Event Feedback: Scenario Example

Email injects containing a potential Cyber Security Incident were sent to participants to try and elicit their theoretical incident response. Discussion questions were also provided to facilitate some general discussion

Inject Example:

- "The SOC receives an alert from the MS-ISAC. The alert indicates unusual traffic patterns from your agency's primary file server.
- Quick internal checks reveal that an attacker has exploited a zero-day vulnerability in Cisco Adaptive Security Appliance (ASA) and Cisco Firepower Threat Defense (FTD) that allows them to gain initial access to the COV (Commonwealth of Virginia) domain. The sophistication suggests it might be a coordinated attack rather than a casual hacker's work.
- Preliminary findings indicate data exfiltration. The exact data sets and the depth of the breach remain uncertain, but given the server's critical role, the potential impact is significant."

Discussion Question Examples:

- "What are the most effective controls against zero-day vulnerabilities?"
- "Are you familiar with the COV vulnerability reports and maintenance?"
- "Does your organization have readily available actions to mitigate zero-day vulnerabilities?"

Event Feedback: Strengths

Scenario injections were both well-received and were believed to be engaging and reflective of the COV IT environment and capture some of the focal points that all agencies should be prepared for.

The format for the virtual Tabletop Exercise this year was well received based on participant's feedback. The number of injects presented and the tempo of the injects kept participants more engaged than previous years.

The discussion questions following each inject allowed participants to consider additional perspectives and components evaluating each inject.

Responses from participants met and/or surpassed expectations. This indicates participants have an extensive comprehension of how Incident Response process works across the COV IT infrastructure.

Event Feedback: Areas for Improvement

Improvement identified: Some participants indicated a need for a more hands on exercise that allows organizations to work together in a group setting.

- **Key Recommendation:** Inter-agency discussion in a smaller group setting will promote knowledge sharing.

Improvement identified: Some participants felt the injects would be more informative if they were more specific to their organization or agency.

- **Key Recommendation:** Modify injects to include agency-specific information/tasks to create a more inclusive exercise.

Improvement identified: Some participants indicated a need to conduct a tabletop exercise more frequently.

- **Key Recommendation:** Conducting a tabletop exercise more frequently would give agencies the ability to review and update their Incident Response policies as environments change.

Additional SIRT Information

Reporting Potential Security Incidents:

1. All Cyber Security Incidents must be reported via the Cyber Incident Form
   - May also call the Virginia Fusion Center at 804-674-2196 or 877-4VA-TIPS

2. If immediate assistance is needed, you may also report issues via the VCCC Helpdesk*
   - Phone: (866) 637-8482
   - Email: vccc@vita.virginia.gov

   *Self-Service is not recommended for issues requiring escalation

Tracking/Reviewing Security Incidents:

- Archer serves as the central location for all COV Security Incidents
  - Incident tickets will show as INC-XXXX and are only accessible to MSI SIRT, ATOS MSS, VITA CSRM and the affected agency ISO's
  - Actions required from non-SIRT teams will typically be tracked via KSE as INC tickets and reported in Archer

Feel free to direct additional questions to:
MSI-Security-Operations@saic.com

Upcoming Events

VIRGINIA
IT AGENCY
vita.virginia.gov

SAVE THE DATE!

August 15

Hilton Richmond Hotel, 12042 West

Broad St., Richmond, VA 23233

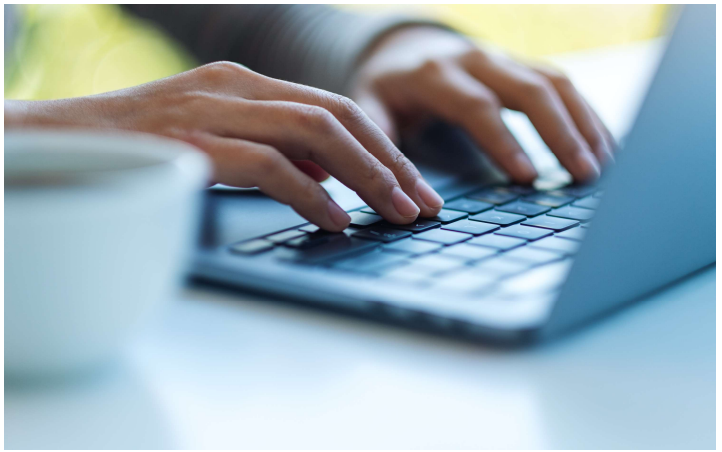
Registration to open soon!

IS Orientation

The next IS Orientation is being held on March 27, 2024

- It will be held virtually via WebEx from 1pm-3pm
- Please register at the link below:

https://covaconf.webex.com/weblink/register/rd212e769bb8f06f1b608aebd01be1cd7



Hybrid ISOAG Meeting

The April 3, 2024 Information Security Officer's Advisory Group will be held both in-person, and remotely via WebEx.

- In-person will be held at VITA, located at the Boulders, seating will be limited to 50 persons and attendees must pre-register. Registration for in-person is on a first come, first served basis. The virtual meeting is open to all.
- For **in-person**, please register at: https://covaconf.webex.com/weblink/register/r87b82b890ceb4dc5cb1e345c753e720e
- For **remote**, please register at the link below: https://covaconf.webex.com/weblink/register/redb8bc29e26e987624b761cd4b7cbd2f

You are a Part of the Program!

VIRGINIA IT AGENCY

Round Table Discussion

For the Hybrid ISOAG Meeting in April we will have a Round Table Discussion. Please be ready and bring your questions!

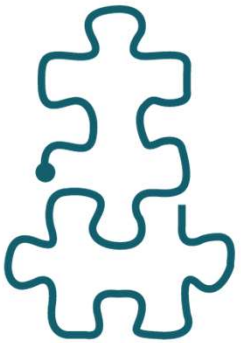
April 5, 2024, ISOAG Meeting

Government Innovation Virginia

Transforming Virginia: Bridging Innovation and Progress

Public Sector Network is presenting: Government Innovation Virginia

- Held on Wednesday, April 17, 2024, at the Downtown Richmond Marriott
- The registration link is below, and attendance is free of charge.
- Government Innovation Virginia 2024 - Public Sector Network



MEETING ADJOURNED

VIRGINIA
IT AGENCY