

**WELCOME TO THE  
July 10, 2024  
ISOAG MEETING**



**VIRGINIA  
IT AGENCY**

**Information Security Officer's  
Advisory Group**

July 10, 2024



## Agenda

## Presenter

Welcome/Opening Remarks

Kendra Burgess/ VITA

COV Grade

Michael Watson/ VITA

An Introduction to ODGA and Unstructured Data Scanning

Jessi Bailey, Chris Burroughs and Imran Afridi / ODGA

Virginia Works Agency

Carrie Roth/VA Works

Update on ISO Manual

Michael Wickham/ VWC

2024 COV Tabletop Exercise

Zachary Wilton/ SAIC

Upcoming Events

Kendra Burgess/ VITA

Adjourn

# Mike Watson

Chief Information Security Officer



VIRGINIA  
IT AGENCY  
[vita.virginia.gov](http://vita.virginia.gov)

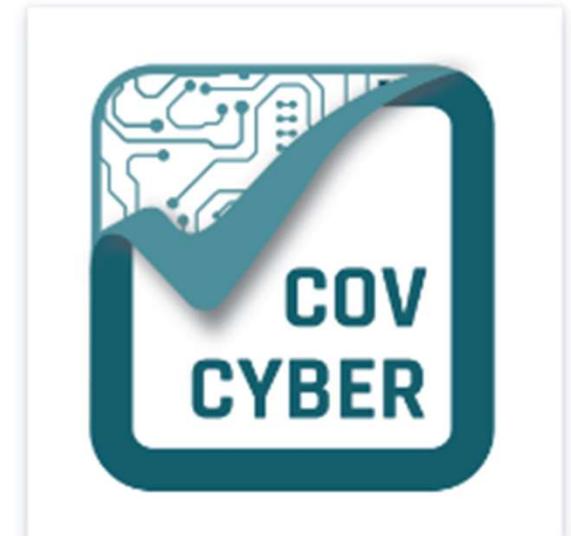
- **COV Cyber**

**The COV Cyber mark signifies trusted and secure cyber products and solutions.**

COV Cyber products will maintain the same level of security that Commonwealth of Virginia customers have come to expect.

Coming soon:

- Over time, each service will be verified through the COV Cyber process
- Managed security services recompetes is underway
- Continue to make updates to dashboards





OFFICE OF DATA  
GOVERNANCE  
AND ANALYTICS



## What We Do

Foster data sharing through the Commonwealth Data Trust

---

Help agencies implement data governance strategies

---

Provide technical assistance

---

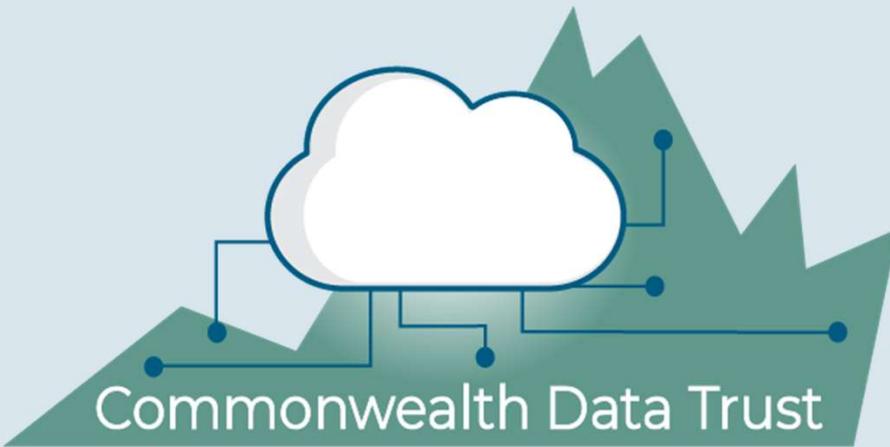
Develop innovative data analysis and intelligence methodologies and best practices to promote data-driven policy making, decision making, research, and analysis





# Commonwealth Data Trust

Standardized, Safe, and Secure Data Sharing



Enables data sharing between agencies

---

Membership provides access to ODGA services and training

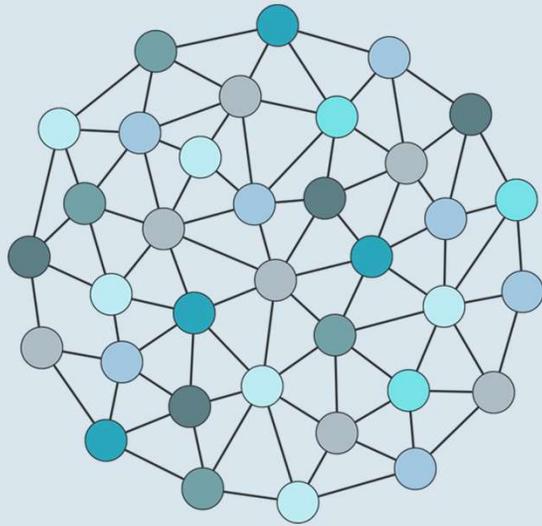
---

No Requirement to contribute data, free to join, not the same as the Workforce Data Trust



# Commonwealth Data Trust

Standardized, Safe, and Secure Data Sharing



Before- Multiple point-to-point, one off agreements

Now- ODGA facilitates safe, secure, and standardized data sharing



**Structured and Unstructured Data Scanning**  
You can't protect data you don't know exists- use our scanning service to uncover PII in your organization

---

**Data Governance Best Practices Consultation**  
We can share policies, procedures, and standards for you to customize to fit your agency

---

**Data Visualization and Analytics Solutions**  
Our Power BI specialists can craft visualizations to enhance patterns, trends, and relationships in your data to enhance patterns, trends, and relationships in your data





# Services: Use Cases

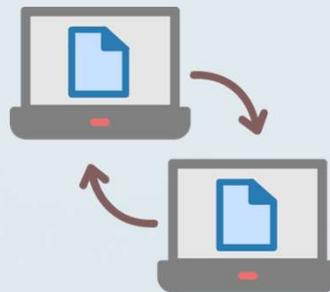
## DVS Veteran Identification

The Department of Veteran Services (DVS) had difficulty identifying all the veterans in Virginia, making outreach and marketing difficult. ODGA implemented a data solution to identify 669,594 Virginian Veterans.



## DBHDS-DMAS Data Sharing

DBHDS regularly requires data from DMAS for a Dept. of Justice report. ODGA facilitated an automatic data sharing process, taking the time needed to fulfill the report from 10 days to 2 days.



## Operation Bold Blue Line

Created Power BI dashboards that showed a variety of violent crime statistics, allowing leaders to make strategic decisions to reduce crime. OBBL resulted in 857 felony arrests and 2,060 pounds of illegal narcotics removed from the street.

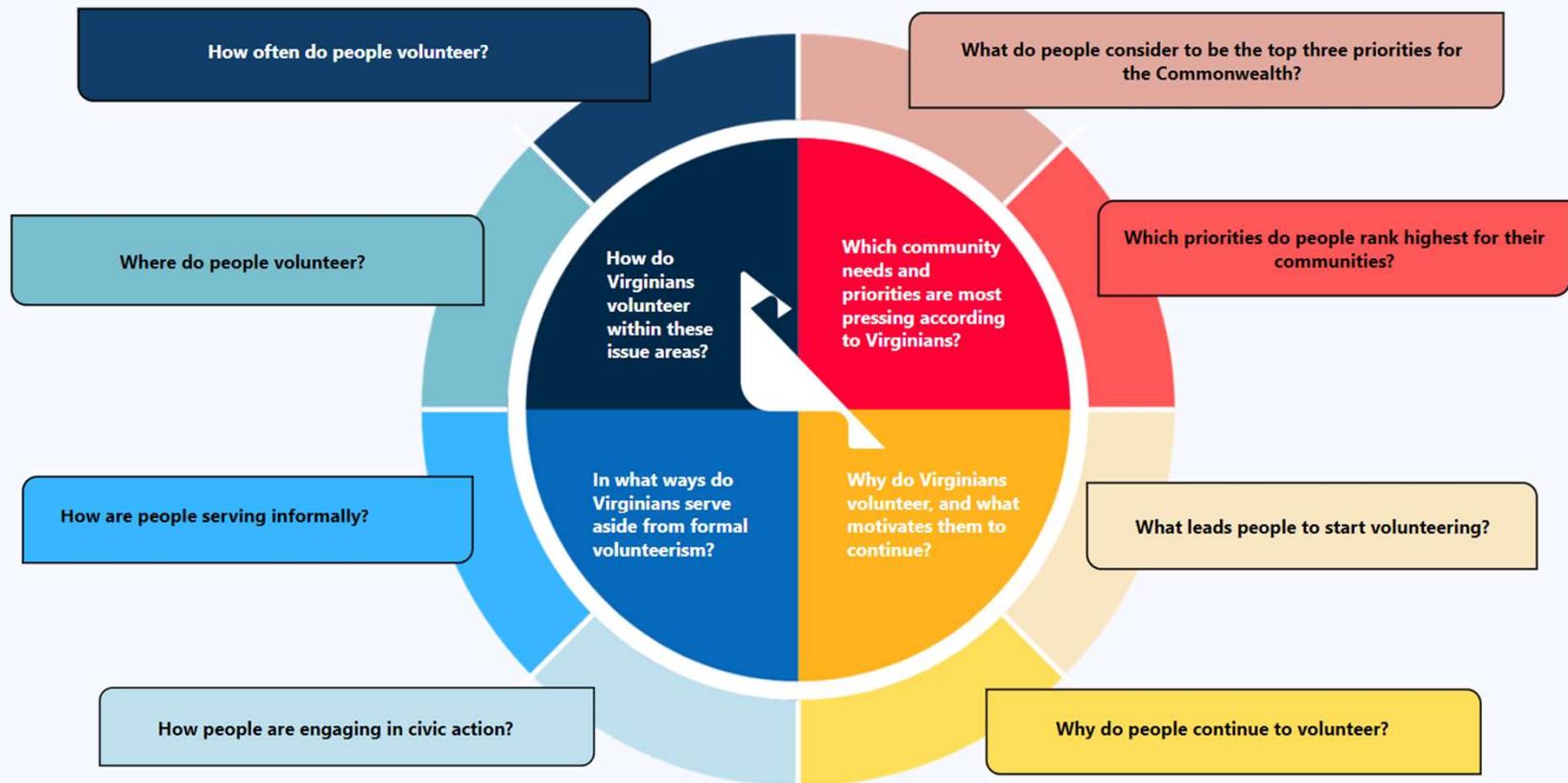




# Power BI Example



## Virginia Community Engagement Index



 | Training

## Data Owner and Data Custodian Training

Available as SCORM file or in the COVLC. Fulfills Sec 527 Requirement

---

## Custom Data Quality Videos (CDT Members Only)

We can create custom videos to tackle data quality challenges specific to your agency

---

## Dataversity (CDT Members Only)

A free license to over 400 data governance training classes and conference sessions, including DM-BOK and CDMP training



Training



# Data Quality Video Example





# Resources

Free on our website

Risk #	Date Opened	Risk Name	Description	Probability	Impact	Priority
						0
						0
						0
						-



## 12 STEPS TO PROTECTING SENSITIVE DATA IN UNSTRUCTURED FILES GUIDEBOOK

Protecting sensitive data in unstructured files requires a combination of technical measures, policies, and practices. Here are some best practices to consider:

- Data Classification:** Start by identifying and classifying sensitive data within unstructured files. Sensitive data includes personally identifiable information (PII), financial data, intellectual property, or any other information critical to your organization.
  - Prioritize your remediation by focusing on the most critical elements first like SSN, credit card number, or clear text passwords.
  - Consider whether sharing sensitive data would be more appropriately stored in databases on servers.

### Data Governance Roles

- Chief Data Officer**
  - Accountable for overall data governance program
    - Focused on mission objectives of agency which may involve looking for cost savings
    - Focused on plan stage of data lifecycle
- Data Owner (Usually Senior Management)**
  - Accountable for ensuring steps are taken to protect data, delegates tasks to data steward.
    - Determines policies, regulatory requirements, compliance needs, and training needed to protect data
- Data Steward**
  - Enforce requirements set by Data Owners
  - Bridge the gap between different data stakeholders
  - Subject matter expert on data and its utility for business use
- Data Custodian (Can Be 3rd Party Supplier)**
  - Oversees storage, transfer, and transport of data
  - Takes care of data and the databases where it's stored
  - Focuses on the "how" instead of the "why" of data storage

## Data Analyst Job Description

### Overview:

We are seeking a talented and detail-oriented Data Analyst to join our dynamic team. As a Data Analyst you will be responsible for interpreting data, analyzing results, and providing actionable insights to support informed decision-making across the agency. You will work closely with stakeholders to understand data needs, develop analytical solutions, and present findings in a clear and concise manner.

### Responsibilities

#### Data Collection and Processing

- Extract, transform, and load (ETL) data from various sources.
- Clean and preprocess data to ensure accuracy and consistency.
- Develop scripts and workflows to automate data collection and processing tasks.

#### Data Analysis and Interpretation:

- Perform exploratory data analysis to uncover trends, patterns, and anomalies.
- Apply statistical and analytical techniques to derive insights from complex datasets.
- Conduct hypothesis testing and predictive modeling to support business objectives.

#### Data Visualization and Reporting

- Create visually appealing and interactive dashboards, reports, and presentations.
- Communicate findings and recommendations to stakeholders using data visualization tools.
- Collaborate with cross-functional teams to design and deliver actionable insights.

#### Data Quality Assurance

- Validate data accuracy, completeness, and integrity.
- Identify and address data quality issues and discrepancies.
- Implement data quality controls and monitoring mechanisms.

# and more!

### Volume

Big data takes up a lot of virtual or physical space with its high volume.

### Variety

Big data contains a large variety of information.

### Velocity



# Virginia Open Data Portal

A platform for agencies to provide data to the public



Open Data Portal

Empowers constituents to turn data into actionable intelligence

---

Signals Government Transparency

---

Data can be downloaded and accessed via API

---

Platform allows for easy searching and filtering capabilities



# Agencies: Get Involved

## Executive Data Board (EDB)

---

Responsibilities include:

- Translate COVA data-driven policy goals and objectives to agency performance targets
- Allocate appropriate agency resources to support data governance, sharing, and analytics initiatives

## Data Governance Council

---

Responsibilities include:

- Liaise between state agency operations and the CDO.
- Advise the CDO on technology, policy, and governance strategies
- Administer data governance policies, standards, and best practices as set by the EDB
- Oversee data sharing and analytics projects
- Review open data assets
- Govern the Commonwealth Data Trust
- Report progress, compliance, and performance to the EDB.

## Data Stewards Group

---

Responsibilities include:

- Promote and facilitate the secure and appropriate sharing and use of data assets in support of data-driven policymaking, evidence-based decision-making, research, and analysis
- Maximize the value and utility of Commonwealth data-related investments and assets
- Provide public access to data assets, where lawful and appropriate, to enhance research, innovation, and insight



# Unstructured Data Scanning Demo

Keeping agencies secure one scan at a time



No data ingestion needed

---

Find where PII is located in agency files

---

Make a plan to properly dispose of or protect PII

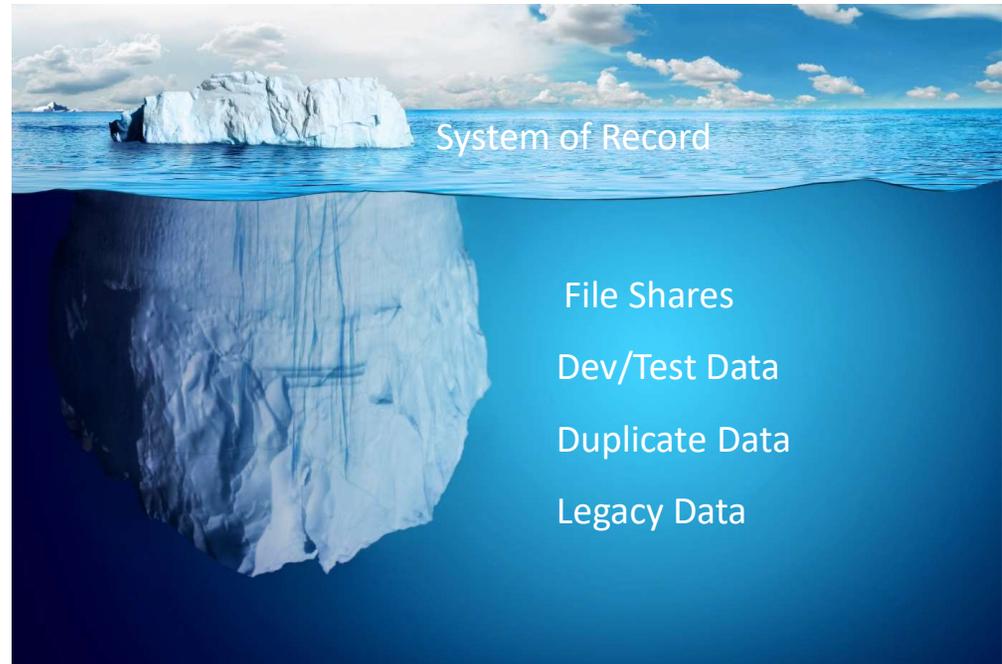
---

Better security for your agency

# Reducing Risk through Unstructured Data Scanning

## Identify Files with:

- Credit Cards
- Passwords in Clear Text
- Drivers License Numbers
- Tax ID's
- Passport Numbers
- PII
- And custom categories



# Pilot Results Show the Unidentified Risk



Clear text passwords & keys



Credit card numbers



Driver's license



Social Security numbers



Bank account numbers



Passport numbers





# BigID Data Coverage

BigID supports a wide variety of data sources with new connectors added regularly

## Structured

- Amazon Athena
- Amazon Redshift
- Azure Active Directory
- CockroachDB
- Databricks
- Google Spanner
- Greenplum
- IBM DB2 (Inc. iSeries)
- IBM Informix
- IBM Netezza
- Microsoft SQL
- MySQL
- Oracle DB
- PostgreSQL
- Presto
- SAP HANA
- SAP Sybase AES
- Snowflake
- Teradata
- Yellowbrick

## Unstructured

- Amazon WorkDocs
- Alibaba Cloud OSS
- Amazon EFS
- Amazon S3 / On-Premise
- Azure (Blob/File Storage)
- Box
- Documentum
- Docusign
- Dropbox
- Google Cloud Storage
- Google Drive
- iManage Drive
- Microsoft Exchange
- Microsoft OneDrive
- Microsoft SharePoint
- Microsoft SharePoint Online
- NFS (Unix/Linux)
- OpenText
- SFTP (Unix/Windows)
- SMB (Windows shares)

## Big Data

- Amazon DocumentDB
- Amazon DynamoDB
- AstraDB
- Azure Cosmos DB
- Azure Data Lake Storage (ADLS)
- Azure File Storage
- Azure Synapse Analytics
- Cassandra
- Couchbase
- Elasticsearch
- Google BigQuery
- Google BigTable
- Google Datastore
- Google Filestore
- Hadoop HAWQ
- Hadoop
- Hbase (Apache)
- Hive
- IBM VSAM
- KDB+
- MarkLogic
- MongoDB / MongoDB Atlas
- Redis
- Splunk
- Vertica

## Business Applications

- AHA!
- Bitbucket Cloud
- Bullhorn
- Confluence
- GitHub Cloud/On Prem
- GitLab
- Gmail
- IBM FileNet
- Iterable
- Jira
- LDAP
- Localytics
- Microsoft Dataverse
- Microsoft Dynamics CRM
- Microsoft O365 Cal/Cont
- Microsoft Outlook
- Microsoft Teams
- MicroStrategy
- Oracle CX Sales
- Oracle Eloqua
- Oracle NetSuite
- Salesforce
- Salesforce Marketing Cloud
- SAP Business Suite
- SAP SuccessFactors
- SAS
- ServiceNow
- Sharefile
- Slack
- Slack Enterprise Grid
- Slack Files
- Tableau
- Workday / WQL
- Zendesk

## Secondary Sources

- SAP Data Hub
- IBM Guardium
- CSV File Import

## Data in Motion

- Kafka
- Kinesis

## Premium Connectors

Platinum Connectors

Gold Connectors

<https://bigid.com/data-coverage/>

# Use Cases

7/10/2024

- Reduce security risk through identification and remediation
  - Auto classify data based on sensitivity
    - Tag SSN, Credit Card # etc with "Restricted/Regulatory"
    - Tag [project name] with "Confidential"
  - Import classifications into Purview for M365 for DLP purposes
  - Produce malware risk assessments
  - Conduct AI impact assessments
- 

# Appendix

## Controls

Commonwealth Data Trust

Change Management

Role-based Access

- Agencies can only view their data
- Preview option turned off by default

Detailed Logging



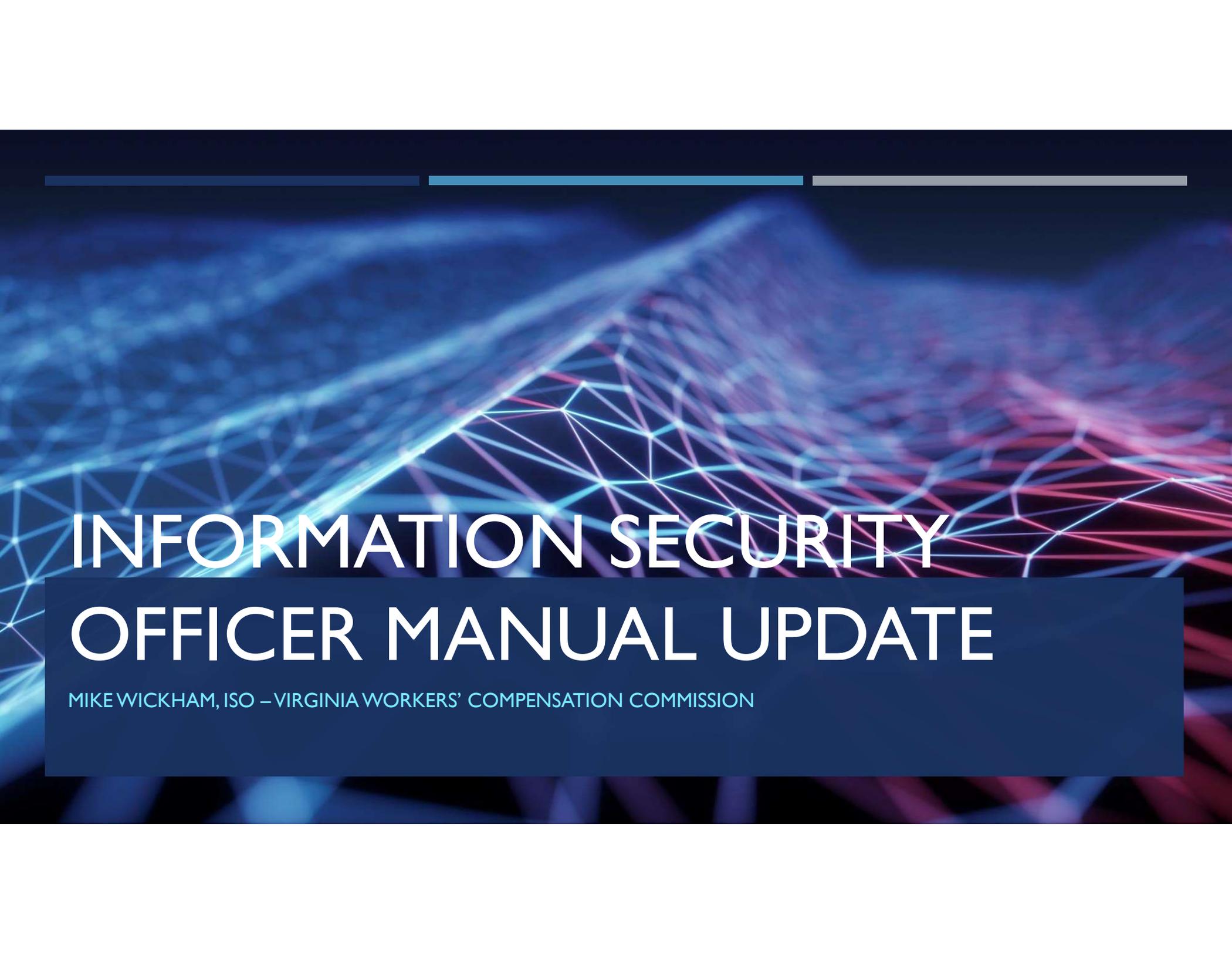


---

DEPARTMENT  
OF WORKFORCE  
DEVELOPMENT  
AND ADVANCEMENT

**Carrie Roth,**  
**Commissioner**

[Virginia Works - Virginia's Workforce Development Agency](#)



# INFORMATION SECURITY OFFICER MANUAL UPDATE

MIKE WICKHAM, ISO – VIRGINIA WORKERS' COMPENSATION COMMISSION

## AGENDA – THE 5 W’S

- How did we get here?
- Why do we need a manual?
- What’s included in this revision?
- When will the manual be ready?
- Where do we find the revised manual?
- Who was involved in this revision?

## HOW DID WE GET HERE?

- 2013 – Information Security Manual was developed.
- 2022 – Information Security Officer Council created a subcommittee to review and revise the ISO manual.
- 2022 – 2024 – ISO Council subcommittee met revising the manual.
- 2024 – Draft completed and is in final review before it is sent to the ISO council for review.

## WHY DO WE NEED A MANUAL

- Manual is written for newly appointment ISOs.
- Seasoned ISOs can also find benefits from the manual.
- Gives a single location for ISOs to gather pertinent information associated with their job functions.
- It's a living document. The document will be updated to provide current information when significant changes are made to ISO responsibilities.

## WHAT'S INCLUDED IN THIS REVISION

- Things a new ISO should do immediately once hired.
- The Supporting Cast – Security Roles and Responsibilities.
- Commonwealth's Information Security Governance Structure.
- Applying the Standards to Build the Program.
- Security Program Details.

## WHAT'S INCLUDED IN THIS REVISION CONTINUED

- Additional ISO Duties - Agency Compliance Requirements
- Tools of the Trade
- Putting it all together
- Helpful Links

## WHEN WILL THE MANUAL BE READY?

- The manual is currently under final review with the committee
- Next it will be sent to the ISO Council for review.
- Target release date is Q3 2024

# WHERE DO WE FIND THE REVISED MANUAL?

The screenshot shows a SharePoint page for 'VITA Connections' with the following content:

- Page Title:** Commonwealth Security and Risk Management (CSRM)
- Introductory Text:** VITA security teams are committed to protecting the Commonwealth's valuable data assets and providing a safe, secure technology environment that enables state agencies to accomplish their respective missions. VITA's security and risk management directorate is tasked with fulfilling this mission and in doing so, offers significant benefits to agencies of the Commonwealth. The team responds to over 30 million cyberattack attempts and blocks more than half a million pieces of malware on the Commonwealth's network every year.
- Announcements:**
  - Registration now open for 2024 security conference:** For awareness: The annual security conference will be held Thursday, Aug. 15 at Hilton Richmond Hotel in Short Pump, with Kamba Wilden as our featured keynote...
  - March 2024: Top 5 critical vulnerabilities:** The Top 5 critical vulnerabilities that have been identified for March 2024 are as follows: 1. Oracle Global Lifecycle Management (iPatch) (Jan 2023 CPU) 2. Telerik UI for...
  - In progress: COV Ota environment changes:** Action required: VITA, along with the identity access management provider, iNtix, are providing live updates regarding the Commonwealth of Virginia (COV) Ota...
  - Reminder: Complete the 2023 National Cyber Security Risk Assessment by February 28th:** To SOC: As we approach the deadline, this is a friendly reminder for all Information Security Officers to complete the 2023 National Cyber Security Risk Assessment (NCSA...
- Spotlight:** A purple banner with the word 'Ardea' partially visible.
- Patch deployments:** A graphic showing a network of nodes and connections.
- CSRM Events:**
  - JUL 10:** ISAG meeting, Wed, Jul 10, 1:00 PM
  - AUG 7:** ISAG meeting, Wed, Aug 7, 1:00 PM
  - AUG 15:** COV Security Conference, Thu, Aug 15, 9:00 AM
  - SEP 11:** ISAG meeting, Wed, Sep 11, 1:00 PM
- Navigation/Tools:** Information Security, Archer, Archer User Guide, Report a Cyber Incident, Suggestions for CSRM.

## WHO WAS INVOLVED IN THIS REVISION?

- Paige Brothers – Department of Corrections
- Renea Dickerson – VITA
- Tina Gaines – VITA
- Derek Kestner – Supreme Court
- Nick Kuriger – Virginia State Bar
- Mike Wickham – Virginia Workers Compensation Commission

# COV Tabletop Exercise 2024

Zachary D. Wilton  
SAIC MSI Security Incident Response

**SAIC**<sup>®</sup>  
Redefining Ingenuity

---

## WHAT TO EXPECT

- Various scenarios, that will require some type of incident response, will be provided to the participants
- Participants will have time to internally discuss and write up their response before providing it to the planning team via email
- There will be also be several optional questions, tips, interesting facts, and other discussion points provided to review all types of topics adjacent to the Incident Response process
- CPE's will be provided for active participants, and it is a great opportunity to interact with other cyber security experts that are part of the COV, as well as asking any questions about the IR process!

---

## EVENT INFORMATION

- **When:**

- Exercise is Thursday, August 8<sup>th</sup>, 2024 from 9AM-3PM
- Hotwash is Friday, August 9<sup>th</sup>, 2024 from 11AM-12PM

- **Who:**

- Hosted by MSI SIRT team, ATOS Security, and VITA CSRM
- Participants include representatives from each agency and service tower (Last year had over 50)

- **Where:**

- Virtual only event - A link will be provided to those that RSVP on

---

## EVENT INFORMATION

- How to join:

- You are always welcome to send an email to [MSI-Security-Operations@saic.com](mailto:MSI-Security-Operations@saic.com) stating that your agency/tower would like to participate in this year's event!
- An email is being sent out via VITA COMMS , with a separate reminder to all STS ISO's
- The full meeting invite for the event will be sent out closer to the event time, once we gather participation
- RSVP Cut-off: **August 2<sup>nd</sup> , 2024 by COB**

**PLEASE DIRECT ALL QUESTIONS ABOUT THE EXERCISE TO  
MSI-SECURITY-OPERATIONS@SAIC.COM**



# Upcoming Events

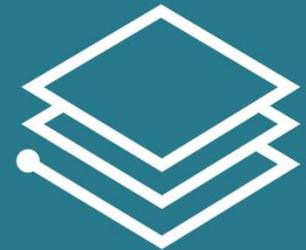


VIRGINIA  
IT AGENCY

[vita.virginia.gov](http://vita.virginia.gov)

## Service Tower SOC Report Review Sessions

The upcoming SOC review session is July 18, 2024, and will be held remotely via WebEx. Please register at the link below



To register for this meeting, please click on the link below:

<https://covaconf.webex.com/weblink/register/r79ff348f2d49da7f1cc45197d77c5b07>



## ISOAG Meeting: August 7, 2024

Presenters: (subject to change)

Darrell Raymond / MSI

Joshua Jones / VITA

Matthew Steinbach / VITA

Please register at the link below:

<https://covaconf.webex.com/weblink/register/r5f2e22c66fbc37943a54ffe3ac16da88>



# Commonwealth of Virginia Information Security Conference 2024

43

Join us for the COV IS Conference 2024

**Titled: “The Art of Cyber War”**

- August 15, 2024, at the Hilton Richmond Hotel and Spa located at Short Pump:  
12042 West Broad Street,  
Richmond, VA 23233

[Register at:](#)

<https://www.vita.virginia.gov/information-security/security-conference/>



# COV IS Conference

**2024 The Art of Cyber War**

**What to expect**



# COV IS Conference Speakers

## Keynote Speakers



[Kemba Walden](#)  
President  
Paladin Global Institute



[Ariyan Bakhti-Suroosh](#)  
Security Consultant II in Optiv's Threat Management practice on the Attack and Penetration Team

## COV IS Conference Speakers

- Great presentations and networking with your peers
- Leadership and technical tracks
- VITA informational sessions where you can meet and interact with representatives from CSRM
- Meet and greet the COV Conference Suppliers/Vendors
- Hands on Lock picking fun

To view the conference program:

<https://www.vita.virginia.gov/information-security/security-conference/conference-program/>

Subject to Change

# Security Services Fair

August 20<sup>th</sup> we will have a **Centralized Information Security Services Fair**



Address: 7325 Beaufont Springs Drive, Richmond,  
VA 23225



# Acunetix 360 Lunch & Learn

Join us at the Boulders on August 29<sup>th</sup>.

Training is onsite only and space is limited. First come first served.

Register at <https://forms.office.com/g/Baku6kYb4f>

Join us for the first Acunetix 360 lunch and learn happening in August. We plan to cover major use cases and settings to ensure you get the highest quality scans and insights into your applications. Topics for the first lunch and learn include:

- How to configure a scan.
- How to create an authenticated scan.
- Scan scoping.
- Retesting for remediation.
- Understanding the resources Acunetix provides to help with remediation.



# Splunk Lunch & Learn – Investigating with Splunk

Join us at the Boulders on September 5<sup>th</sup>.

Training is onsite only and space is limited. First come first served.

Register at <https://forms.office.com/g/WmNiWQc1Dt>

Investigating with Splunk is a modular, hands-on workshop designed to familiarize participants with how to investigate incidents using Splunk and open source. This workshop provides users a way to gain experience searching in Splunk to answer specific questions related to an investigation. These questions are similar to what would be asked in their own organizations. The workshop leverages the popular Boss of the SOC (BOTS) dataset in a question and answer format. Users will leave with a better understanding of how Splunk can be used to investigate in their enterprise.



- **SPLUNK UPDATE JUNE 2024**



## **WE WANT YOUR LOGS:**

**VITA is starting to work with agencies to ingest their application logs in to the VITA Splunk instance. We ask that all agencies start identifying what logs you would like to have ingested. We are always happy to schedule a call to review your options.**

» COVITS

# Save the Date!

September 11 / Richmond, VA

20  
24

# COVITS



[Registration link.](#)



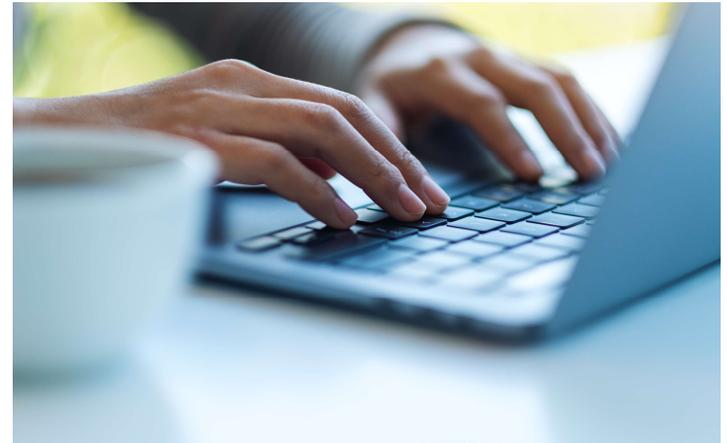
[vita.virginia.gov](http://vita.virginia.gov)

# IS Orientation

The next IS Orientation is being held on September 25th

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

<https://covaconf.webex.com/weblink/register/ra80c2228f9b560704b5193640d78b1a5>



## October 2<sup>nd</sup> ISOAG

**The Mandatory October 2, 2024, ISOAG meeting will be an In-person/Hybrid Event**

**Location will be the Reynolds Community College**

**In the Workforce Development and Conference Center**

This is an opportunity to catch up with your fellow Information Security Officers in person, enjoy informative presentations, and mingle. Seating is limited to 150, so reserve your place at the in-person event. If you are unable to attend in person, and need someone to attend in your place, please notify Commonwealth Security, as attendance is mandatory for ISO's.

Link to register in person:

<https://covaconf.webex.com/weblink/register/r0809a97ccffc9550fed4f1325179cb89>

Link to registers remote:

<https://covaconf.webex.com/weblink/register/r527efc3bfe8a72d8eb29a04d0b988714>



1651 East Parham Road  
Richmond, Virginia 23228

[vita.virginia.gov](http://vita.virginia.gov)

**MEETING  
ADJOURNED**



VIRGINIA  
**IT AGENCY**

ISOAG July 10, 2024

