WELCOME TO THE ISOAG MEETING

VIRGINIA IT AGENCY

Information Security Officer's Advisory Group

July 9, 2025

VIRGINIA IT AGENCY

Agenda	Presenter
Welcome/Opening Remarks	Wesley Dupree/VITA
2025 Cyber Threat Landscape	Christopher Cope/FBI
Updated Standards	Amy Braden/VITA
Intro to Virginia Office of Data Governance and Analytics	Jessi Bailey, Chris Burroughs, Chris Wooten/ODGA
TLS 1.0/1.1 Remediation	John Del Grosso/VITA
Server Vulnerability Compliant Patching Schedule	John Del Grosso/VITA
Upcoming Events	Wesley Dupree/VITA
Adjourn	

SLIDES INTENTIONALLY OMITTED/ SLIDES REDACTED DUE TO SECURITY

2025 Cyber Threat Landscape

Christopher Cope/FBI

ISOAG MEETING

JULY 9, 2025

VIRGINIA
IT AGENCY

SEC540 Data Classification Standard

Director, IT Security Governance & Compliance

Amy Braden

Data Classification Standard SEC540

SEC540 identifies and defines minimum data classification labels to use when classifying data. It also provides labels for data subject to regulatory compliance requirements (e.g., FTI, PHI) and special considerations such as test AI data.

SEC530 language and controls related to data classification have also been updated with references to SEC540.

VIRGINIA IT AGENCY | odga Office of Data Governance and Analytics

Intro to Virginia Office of Data Governance and Analytics

Director of Data Governance Chris Burroughs, Director or Architecture and Engineering Chris Wooten, and Data Engagement Manager Jessi Bailey

ODGA- 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

Boards and councils

Executive Data Board (EDB)

- High-level leadership
- Drive data-driven policy goals

Data Governance Council (DGC)

- Employees of agencies represented on EDB
- Advise CDO on technology, policy, and governance strategies

Data Stewards Group (DSG)

- Employees from executive branch agencies with technical expertise in data management/analytics
- Focuses on executing the high level strategies determined by the EDB and DGC

ODGA: now an office within VITA

From General Assembly 2025 House Bill 1632 & Senate Bill 1137:

"There is created in the Virginia Information Technologies Agency the Office of Data Governance and Analytics to foster and oversee the effective sharing of data among state, regional, and local public entities and public institutions of higher education, implement effective data governance strategies to maintain data integrity and security, and promote access to Commonwealth data. The Office shall be overseen by the Chief Information Officer of the Commonwealth as a part of the Virginia Information Technologies Agency but led in strategy and prioritization by the Chief Data Officer, as established pursuant to § 2.2-203.2:4."

What’s the difference?

VITA:

1.Cybersecurity: Protect people, assets and information from loss, damage and misuse

2.Infrastructure: Ensure the operating environment is efficient, secure, available, and delivers the best value

3.Governance: Provide policy and standards for technology, best practices, cybersecurity, project management, and enterprise optimization

4.Procurement: Develop value-driven statewide IT contracts that enable Commonwealth public bodies to obtain the best value for their organizations
 ($1B+ annually with ~ 1/3 being used by localities)

ODGA:

1.Data Governance: Providing guidance, templates, and tools so agencies know what data they have, where it is located within their environments and how to best manage, upkeep, and protect those datasets.

2.Data Sharing: Providing a safe, secure data sharing process for agencies in the Commonwealth (Commonwealth Data Trust).

3.Data Management: Providing a technical environment to assist agencies with the storage, reporting, and analytics of their data, empowering them to gain actionable insight to make decisions.

Working with agencies: Commonwealth Data Trust

Standardized, Safe, and Secure Data Sharing

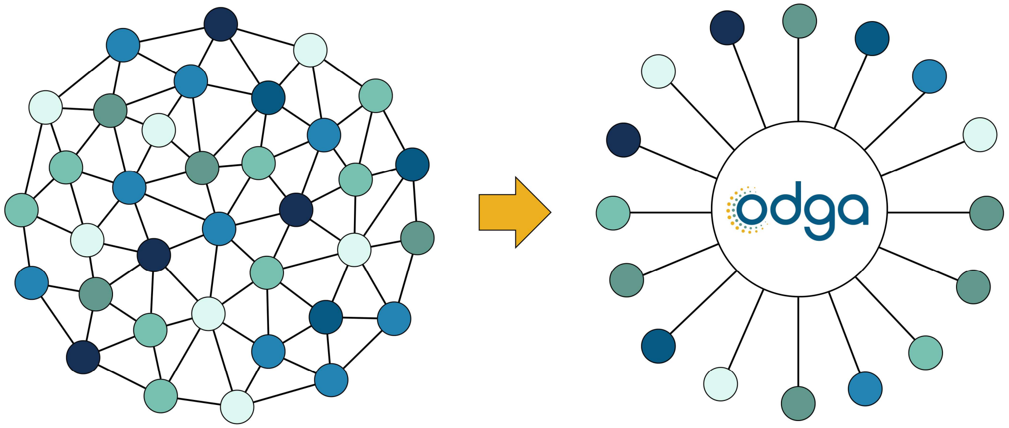
- Enables data sharing between agencies
- Membership provides access to ODGA services and training
- No Requirement to contribute data, free to join, not the same as the Workforce Data Trust

COMMONWEALTH DATA TRUST

Working with agencies: Commonwealth Data Trust pt 2.

The Commonwealth Data Trust (CDT)

A scalable alternative to multiple “point-to-point” sharing



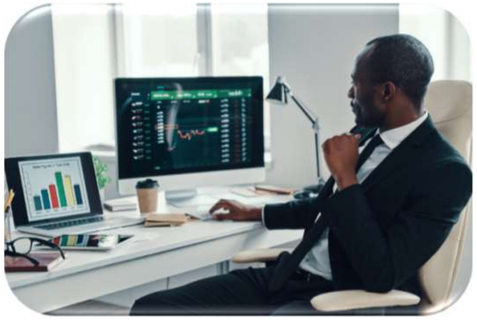
Before the CDT: Agencies shared data through one off agreements

After the CDT: ODGA acts as a conduit to facilitate a safe, secure, and standardized data sharing process

Services: Engineering and Infrastructure Team

Data Collection and Integration

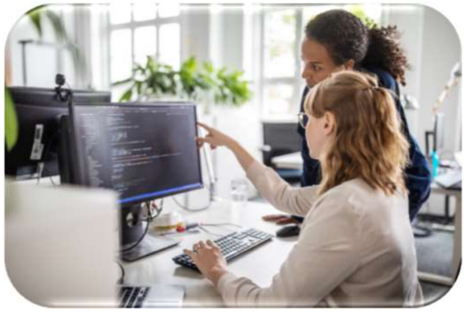
Interagency Data Sharing



Custom Data Modeling, External Data Feeds and Export

Business Intelligence Reporting and Dashboards

Data Engineering Services



Custom Software Development

VIRGINIA IT AGENCY

odga Office of Data Governance and Analytics

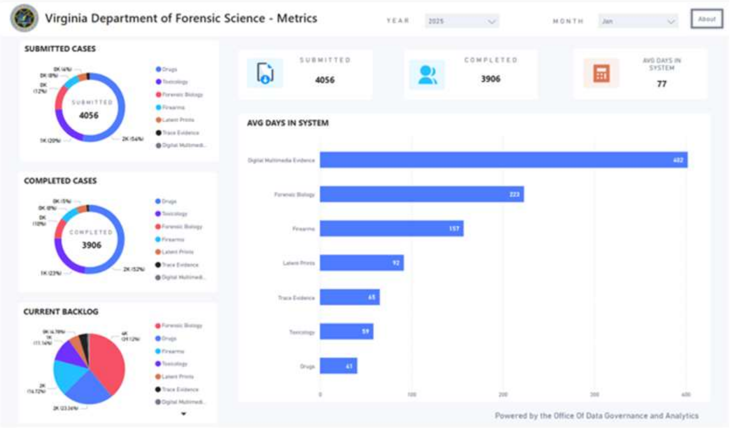
Power BI dashboards

- Design and build interactive dashboards tailored to agency reporting needs.
- Connect to a wide range of data sources, including hosted systems and external datasets.
- Enable self-service analytics and on-demand data exploration.
- Visualize complex data through intuitive charts, maps, and KPIs.
- Ensure data accuracy and consistency through centralized data models.
- Improve decision making with up-to-date insights and performance monitoring.
- Secure data access through role-based permissions and integration with Entra ID.

Power BI dashboard examples

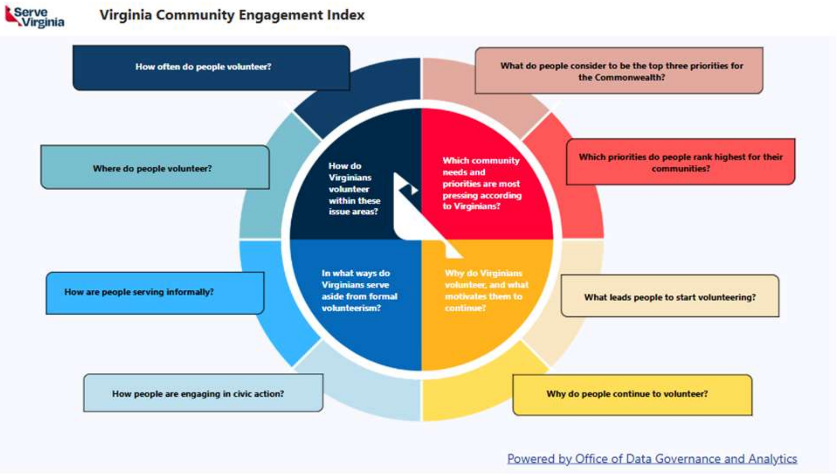
Department of Forensic Science Case Statistic Dashboards

- Provides information about DFS case types including biology, trace evidence, digital multimedia evidence, firearms, latent prints, toxicology, drugs, and questioned documents.



Serve Virginia

- Helped Serve Virginia team compile extensive results from a survey
- Provided necessary Power BI expertise to Serve Virginia team.


Virginia Community Engagement Index

Serve Virginia
How often do people volunteer?
What do people consider to be the top three priorities for the Commonwealth?
Where do people volunteer?
Which priorities do people rank highest for their communities?
How do Virginians volunteer within these issue areas?
Which community needs and priorities are most pressing according to Virginians?
In what ways do Virginians serve aside from formal volunteerism?
Why do Virginians volunteer, and what motivates them to continue?
How are people serving informally?
What leads people to start volunteering?
How people are engaging in civic action?
Why do people continue to volunteer?

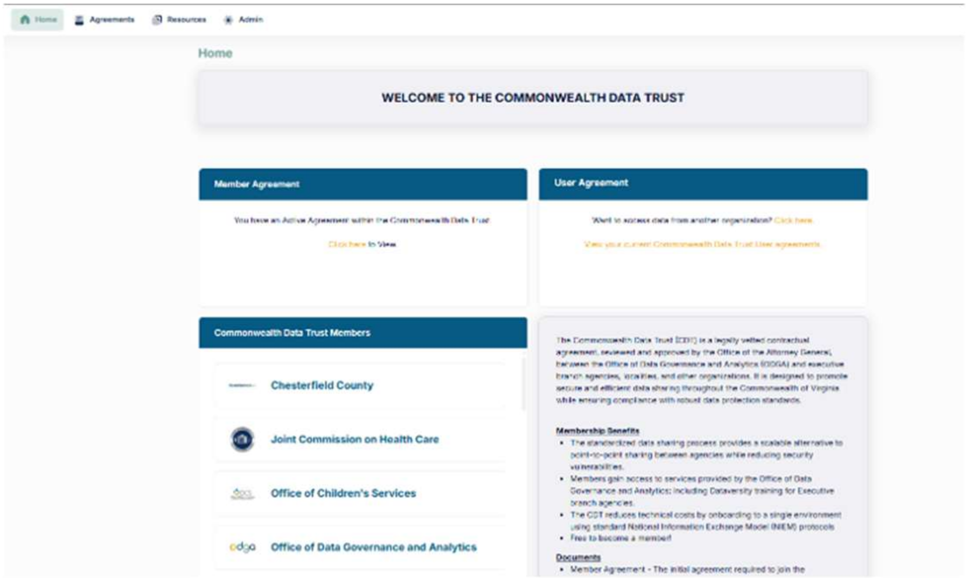
Powered by Office of Data Governance and Analytics

Agency data hosting capabilities

- Provide secure, scalable cloud infrastructure for hosting agency data or applications.
- Enable agencies to leverage ODGA managed Azure resources without having to maintain their own cloud footprint.
- Ensure compliance with Commonwealth security and data governance policies.
- Manage all aspects of hosting: provisioning, monitoring, patching, backups, and access control.
- Support integration with other agency systems, analytics platforms, and reporting tools.
- Enable cross-agency data sharing through centralized hosting.

Custom software development

- Design and develop tailored software solutions to support internal business processes.
- Automate manual workflows to improve operational efficiency across ODGA.
- Leverage modern development frameworks and secure cloud-based architectures.
- Build reuseable components with scalability in mind for future agency use.
- Position ODGA to offer custom development services to other agencies in the future.
- Reduce the need for external vendors by providing in-house expertise.



WELCOME TO THE COMMONWEALTH DATA TRUST

Member Agreement

You have an Active Agreement within the Commonwealth Data Trust

Click here to View

User Agreement

Want to access data from another organization? Click here

View your current Commonwealth Data Trust User agreements

Commonwealth Data Trust Members

- Chesterfield County
- Joint Commission on Health Care
- Office of Children's Services
- Office of Data Governance and Analytics

The Commonwealth Data Trust (CDT) is a legally vetted contractual agreement, reviewed and approved by the Office of the Attorney General, between the Office of Data Governance and Analytics (ODGA) and executive branch agencies, localities, and other organizations. It is designed to promote secure and efficient data sharing throughout the Commonwealth of Virginia while ensuring compliance with robust data protection standards.

Membership Benefits

- The standardized data sharing process provides a scalable alternative to point-to-point sharing between agencies while reducing security vulnerabilities.
- Members gain access to services provided by the Office of Data Governance and Analytics; including Dataversity training for Executive branch agencies.
- The CDT reduces technical costs by onboarding to a single environment using standard National Information Exchange Model (NIEM) protocols
- Free to become a member!

Documents

- Member Agreement - The initial agreement required to join the

Data engineering/architecture services: use cases

- **Virginia Permitting Transparency**
  - Cross-agency platform to create a unified Permit tracking system. ODGA worked to create data models and Power BI visualizations for the project.
- **DBHDS-DMAS Data Sharing Project**
  - 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.

Services: governance team

Publish Data to the Public

Discover sensitive data

Curate and govern data

Data Quality

Training

Resources

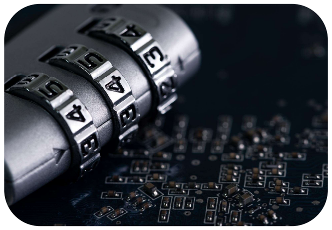
VIRGINIA IT AGENCY

odga Office of Data Governance and Analytics

Governance services: use cases

- **BigID Scanning: Unstructured Data**
  - As of November 2024: 14.75 million files scanned. One agency found files that they didn’t have software to open anymore! Helping agencies eliminate old files, properly classify current files, and potentially save money on storage.
- **COVLC Data Governance Training:**
  - As of November 2024: 14 agencies provided SCORM files and 79 folks completed the training in the COVLC.
- **Commonwealth-Wide Data Catalog:**
  - As of June 2025: 53 agencies have contributed a list of datasets to the Commonwealth Data Catalog. 744 datasets overall, 425 datasets available to view.

Pilot results show the unidentified risk



Clear text passwords & keys

Credit card numbers

Driver's license

Social Security numbers

Bank account numbers

Passport numbers

DBHDS
Virginia Department of Behavioral Health and Developmental Services

DEQ
Virginia Department of Environmental Quality

DCR

OSIG
Office of the State Inspector General
Commonwealth of Virginia

Department of Criminal Justice Services
Virginia

Virginia Department of SBSD
Small Business & Supplier Diversity

Virginia Department of Social Services

Virginia State Police
Valor Service Pride

DGS

Virginia Department of Education

Virginia Tax

Virginia 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

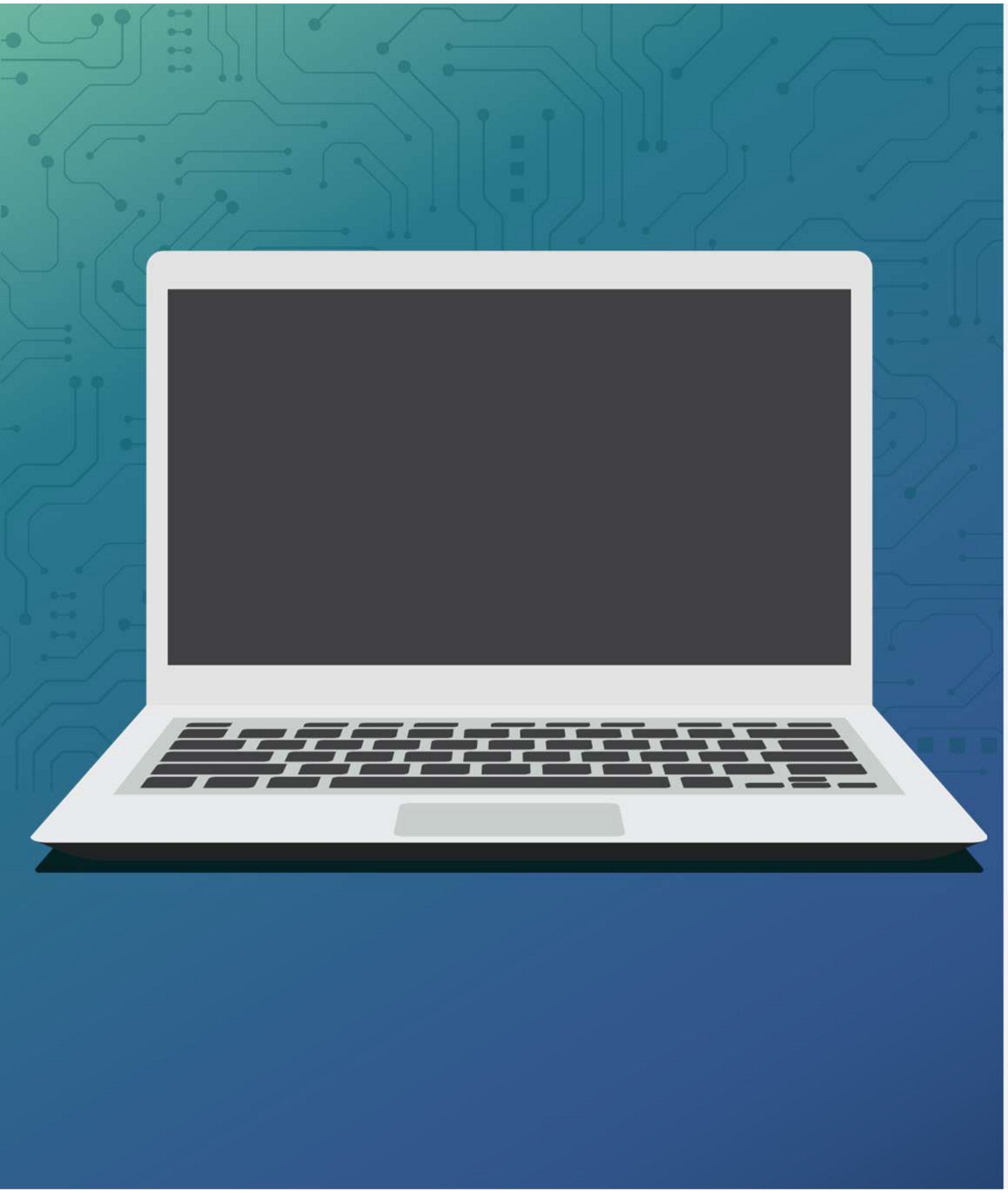
VIRGINIA
OPEN DATA
PORTAL

Key active projects: Substance Use Disorder Abatement

- Cross-agency platform to address Opioid crisis
- Staging in Azure; Production in AWS
- Data Quality profiling using Informatica
- Metadata Management using MS Purview for Data Governance

Key Active projects: Finance Agency Risk Reduction

- MS Purview for Data Governance for structured data
- BigID for unstructured data
- Partnering with CSRM on Data Classification Standard
- Focus on TAX and then work with TRS and DOA



Free resources for agencies

Data governance training: FREE for agencies!

- Data Owner and Data Custodian Training

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

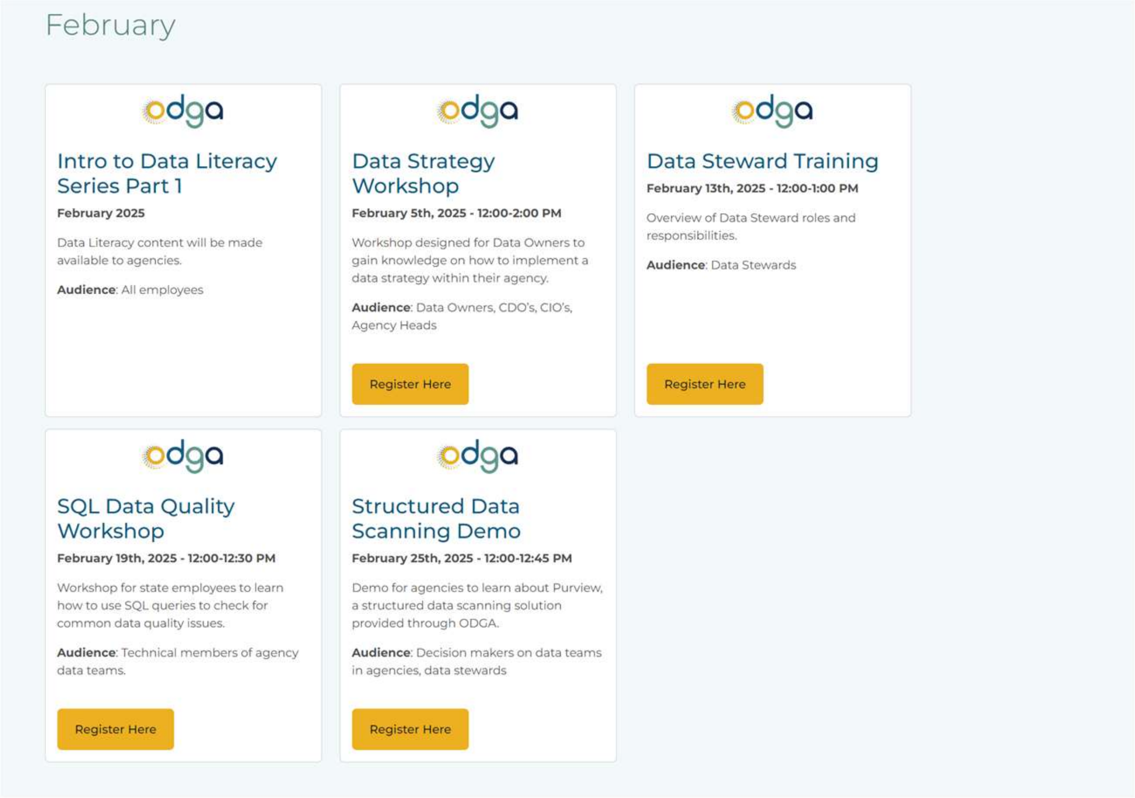
- Custom Data Quality Videos (CDT Members Only)

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

- Dataversity Training (CDT Members Only)

Scholarship to Dataversity website- classes on data governance concepts

Lunch and learn series: FREE for agencies!



February

Intro to Data Literacy Series Part 1

February 2025

Data Literacy content will be made available to agencies.

Audience: All employees

Data Strategy Workshop

February 5th, 2025 - 12:00-2:00 PM

Workshop designed for Data Owners to gain knowledge on how to implement a data strategy within their agency.

Audience: Data Owners, CDO's, CIO's, Agency Heads

Register Here

Data Steward Training

February 13th, 2025 - 12:00-1:00 PM

Overview of Data Steward roles and responsibilities.

Audience: Data Stewards

Register Here

SQL Data Quality Workshop

February 19th, 2025 - 12:00-12:30 PM

Workshop for state employees to learn how to use SQL queries to check for common data quality issues.

Audience: Technical members of agency data teams.

Register Here

Structured Data Scanning Demo

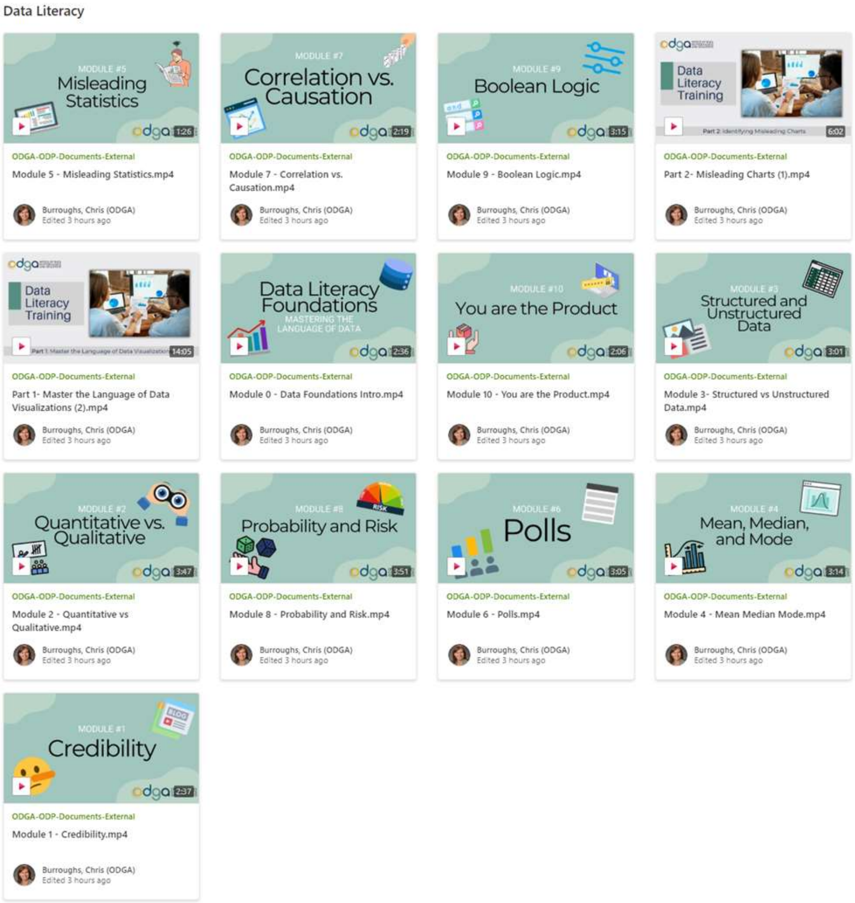
February 25th, 2025 - 12:00-12:45 PM

Demo for agencies to learn about Purview, a structured data scanning solution provided through ODGA.

Audience: Decision makers on data teams in agencies, data stewards

Register Here

Data literacy update: FREE for agencies



Data Literacy

ODGA-ODP-Documents-External
Module 5 - Misleading Statistics.mp4
Burroughs, Chris (ODGA)
Edited 3 hours ago

ODGA-ODP-Documents-External
Module 7 - Correlation vs. Causation.mp4
Burroughs, Chris (ODGA)
Edited 3 hours ago

ODGA-ODP-Documents-External
Module 9 - Boolean Logic.mp4
Burroughs, Chris (ODGA)
Edited 3 hours ago

ODGA-ODP-Documents-External
Part 2- Misleading Charts (1).mp4
Burroughs, Chris (ODGA)
Edited 3 hours ago

ODGA-ODP-Documents-External
Part 1- Master the Language of Data Visualizations (2).mp4
Burroughs, Chris (ODGA)
Edited 3 hours ago

ODGA-ODP-Documents-External
Module 0 - Data Foundations Intro.mp4
Burroughs, Chris (ODGA)
Edited 3 hours ago

ODGA-ODP-Documents-External
Module 10 - You are the Product.mp4
Burroughs, Chris (ODGA)
Edited 3 hours ago

ODGA-ODP-Documents-External
Module 3- Structured vs Unstructured Data.mp4
Burroughs, Chris (ODGA)
Edited 3 hours ago

ODGA-ODP-Documents-External
Module 2 - Quantitative vs Qualitative.mp4
Burroughs, Chris (ODGA)
Edited 3 hours ago

ODGA-ODP-Documents-External
Module 8 - Probability and Risk.mp4
Burroughs, Chris (ODGA)
Edited 3 hours ago

ODGA-ODP-Documents-External
Module 6 - Polls.mp4
Burroughs, Chris (ODGA)
Edited 3 hours ago

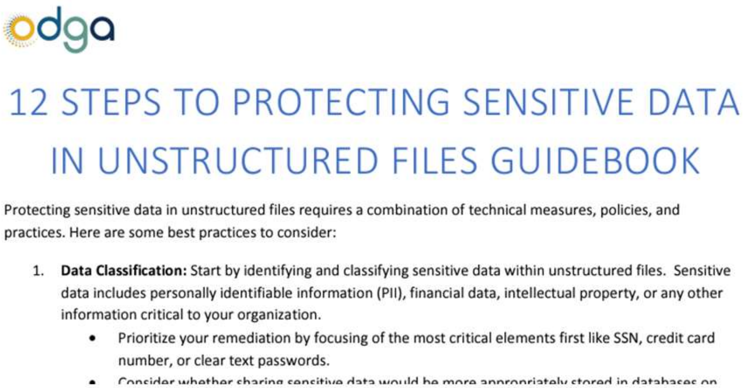
ODGA-ODP-Documents-External
Module 4 - Mean Median Mode.mp4
Burroughs, Chris (ODGA)
Edited 3 hours ago

ODGA-ODP-Documents-External
Module 1 - Credibility.mp4
Burroughs, Chris (ODGA)
Edited 3 hours ago

Resource library: FREE for agencies!

- **Draft Data Classification Policy Templates**
  - Establishes a framework for classifying Commonwealth data based on its sensitivity, criticality, and applicable legal or regulatory requirements.
- **Data Retention Policy Templates**
  - Establishes guidelines for the retention and disposal of data within [Insert Agency]. This policy ensures that data is retained for appropriate periods to comply with legal, regulatory, and operational requirements.
- **Data Security Policy Template**
  - Outlines the principles and procedures for ensuring the security of data within [Insert Agency]. This policy aims to protect the confidentiality, integrity, and availability of data, and to comply with applicable laws.
- **Data Privacy Policy Template**
  - Establishes guidelines for protecting the privacy of individuals' personal information within [Insert Agency].

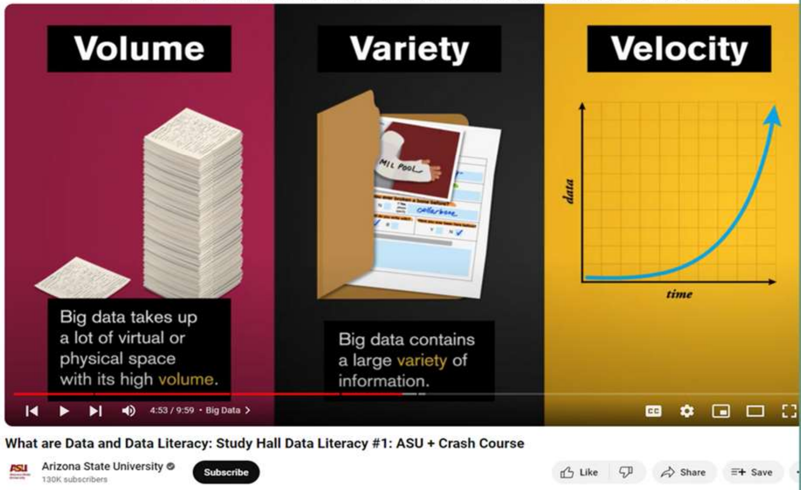
FREE resource library for agencies



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:

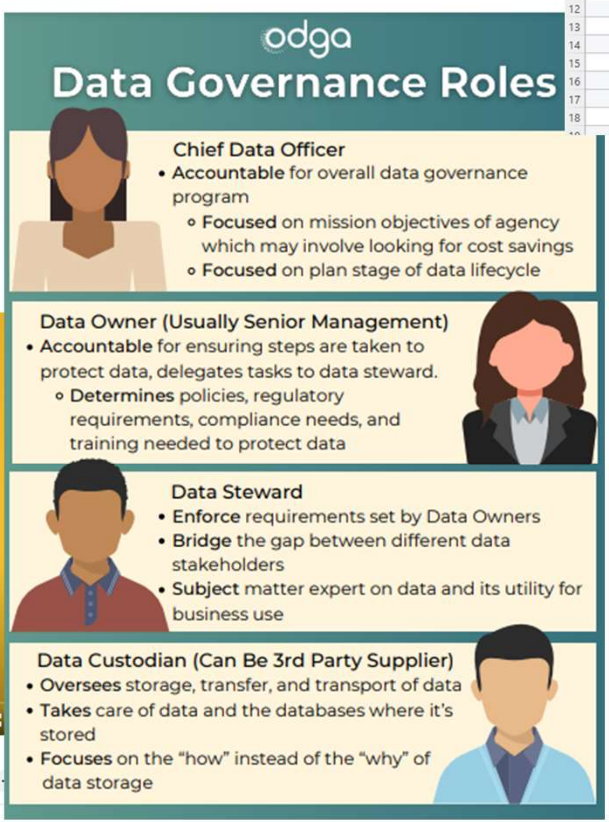
1. **Data Classification:** Start by identifying and classifying sensitive data within unstructured files. Sensitive data includes personally identifiable information (PII), financial data, intellectual property, or any other information critical to your organization.
   - Prioritize your remediation by focusing of 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



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

Big data contains a large variety of information.

What are Data and Data Literacy: Study Hall Data Literacy #1: ASU + Crash Course



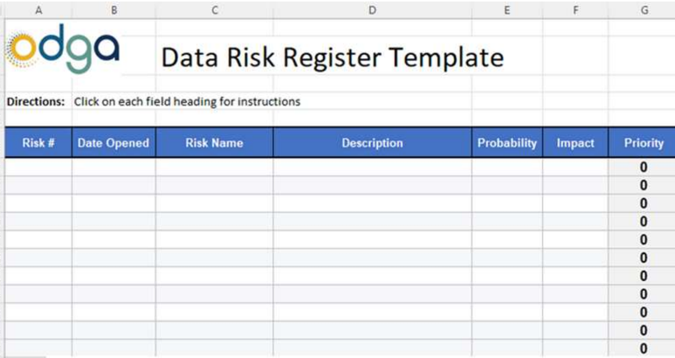
Data Governance Roles

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

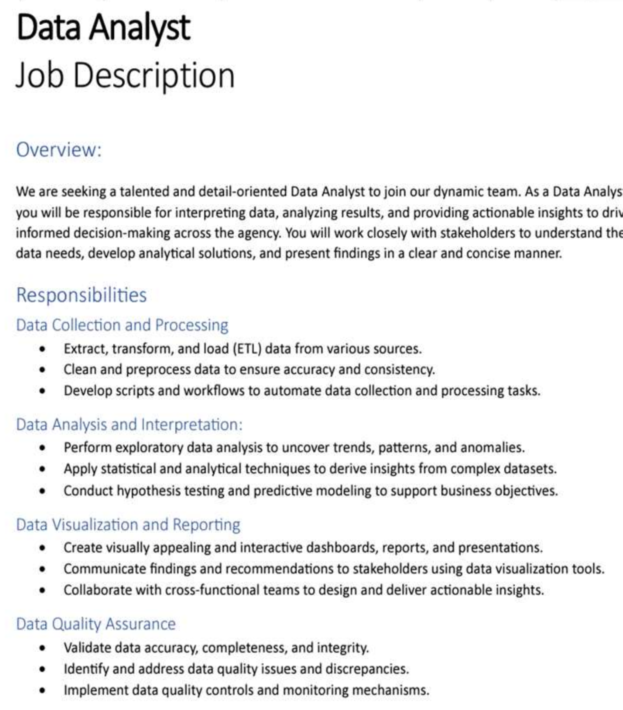
Data Custodian (Can Be 3rd Party Supplier)
- **Oversees** storage, transfer, and transport of data
- **Takes** care of data and the databases where it's stored
- **Focuses** on the "how" instead of the "why" of data storage



Data Risk Register Template

Directions: Click on each field heading for instructions

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



Data Analyst
Job Description

Overview:

We are seeking a talented and detail-oriented Data Analyst to join our dynamic team. As a Data Analys you will be responsible for interpreting data, analyzing results, and providing actionable insights to driv informed decision-making across the agency. You will work closely with stakeholders to understand the 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.

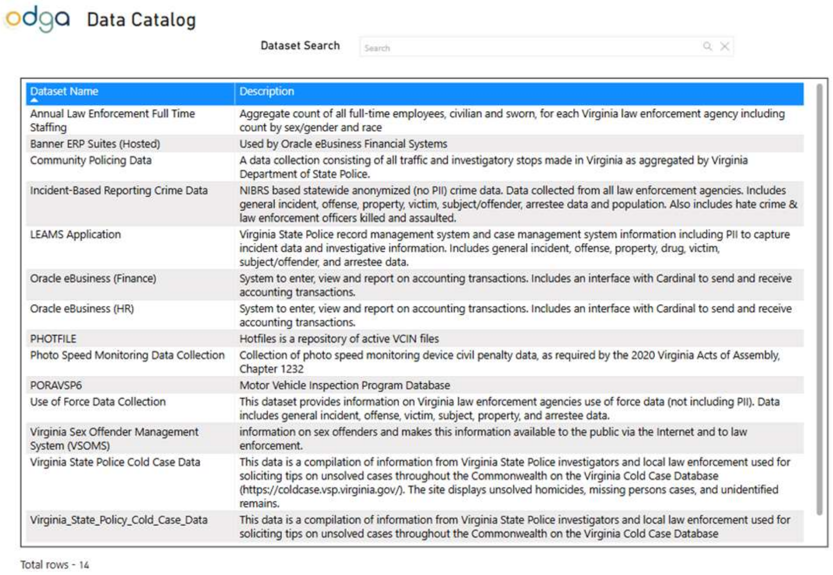
Data Visualization and Reporting
- Create visually appealing and interactive dashboards, reports, and presentations.
- Communicate findings and recommendations to stakeholders using data visualization tools.
- Collaborate with cross-functional teams to design and deliver actionable insights.

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

Commonwealth of Virginia data catalog: FREE for agencies

One stop shop to see a list of agency datasets

- See basic information about datasets, like title and security level
- See the data owner of the dataset to make requests for data
- ODGA will help facilitate data sharing between agencies



odga Data Catalog

Dataset Search

Dataset Name	Description
Annual Law Enforcement Full Time Staffing	Aggregate count of all full-time employees, civilian and sworn, for each Virginia law enforcement agency including count by sex/gender and race
Banner ERP Suites (Hosted)	Used by Oracle eBusiness Financial Systems
Community Policing Data	A data collection consisting of all traffic and investigatory stops made in Virginia as aggregated by Virginia Department of State Police.
Incident-Based Reporting Crime Data	NIBRS based statewide anonymized (no PII) crime data. Data collected from all law enforcement agencies. Includes general incident, offense, property, victim, subject/offender, arrestee data and population. Also includes hate crime & law enforcement officers killed and assaulted.
LEAMS Application	Virginia State Police record management system and case management system information including PII to capture incident data and investigative information. Includes general incident, offense, property, drug, victim, subject/offender, and arrestee data.
Oracle eBusiness (Finance)	System to enter, view and report on accounting transactions. Includes an interface with Cardinal to send and receive accounting transactions.
Oracle eBusiness (HR)	System to enter, view and report on accounting transactions. Includes an interface with Cardinal to send and receive accounting transactions.
PHOTFILE	Hotfiles is a repository of active VCIN files
Photo Speed Monitoring Data Collection	Collection of photo speed monitoring device civil penalty data, as required by the 2020 Virginia Acts of Assembly, Chapter 1232
PORAVSP6	Motor Vehicle Inspection Program Database
Use of Force Data Collection	This dataset provides information on Virginia law enforcement agencies use of force data (not including PII). Data includes general incident, offense, victim, subject, property, and arrestee data.
Virginia Sex Offender Management System (VSOMS)	information on sex offenders and makes this information available to the public via the Internet and to law enforcement.
Virginia State Police Cold Case Data	This data is a compilation of information from Virginia State Police investigators and local law enforcement used for soliciting tips on unsolved cases throughout the Commonwealth on the Virginia Cold Case Database (https://coldcase.vsp.virginia.gov/). The site displays unsolved homicides, missing persons cases, and unidentified remains.
Virginia_State_Policy_Cold_Case_Data	This data is a compilation of information from Virginia State Police investigators and local law enforcement used for soliciting tips on unsolved cases throughout the Commonwealth on the Virginia Cold Case Database

Total rows - 14

How to utilize FREE ODGA resources:

Contact ODGA if you are interested in:

-Data Governance Consultation

-ODGA Data Catalog Access

-Data Owner and Custodian Training SCORM Files

-Dashboards/analytics for Security KPIs

-Cross-agency data sharing

Find on ODGA's website:

-ODGA Resource Library

-Data Governance and Literacy Site

VIRGINIA IT AGENCY | odga Office of Data Governance and Analytics

Thank you!

ODGA Team

odga@odga.virginia.gov

VIRGINIA IT AGENCY

TLS 1.0/1.1 Remediation

Enterprise Project DJ0

John C. Del Grosso

Slide 34

DJ0 I approve the format changes. My edits are complete. Ready to approve.

Delgrosso, John (VITA), 2025-06-26T18:17:59.225

Encryption protocols have gone end-of-life (EOL)

Release	Release date	End-of-life
TLS 1.3	March 2018	Undetermined
TLS 1.2	August 2008	Not yet announced
TLS 1.1	April 2006	June 30, 2018
TLS 1.0	January 1999	June 30, 2018

- Transport layer security (TLS) 1.0 and TLS 1.1 are end-of-life
- All TLSv1.0 and v1.1 must migrate to TLSv1.2 or TLSv1.3

Slide 35

DJ0 Added EOL for TLS1.2/1.3 - to not have blank cells. Based on current projections.

Delgrosso, John (VITA), 2025-06-24T13:09:32.038

Recent activities and discovery

- Security group or policy restricts the change at the operating system (OS) level to restrict the use of TLS 1.0/1.1
  - Changing the setting at OS level requires a re-boot. Upon reboot, the security group or policy resets the policy, so a manual change to revert the rule can never take affect
- Review of 'security hardening' requirements for OS (Windows and Linux) restricts TLS 1.0/1.1 in more recent versions of OS (OS2016 and up, Linux 7 and up)
- Tenable scans show that TLS1.0/1.1 is only being "allowed" on Port 3389 (remote desktop), indicating that server access may be occurring while engineers use tools (browsers, putty, etc.)
- **It doesn't mean that TLS 1.0/1.1 is being used, just that it's an open option to restrict**

What is port 3389: Remote desktop protocol (RDP)

TCP port 3389 is used for remote desktop protocol (RDP), a proprietary protocol developed by Microsoft that allows users to connect to a remote computer over a network connection. If this port is open and accessible to the internet without any restrictions, it can be a major security vulnerability as attackers can exploit it to gain unauthorized access to your system.

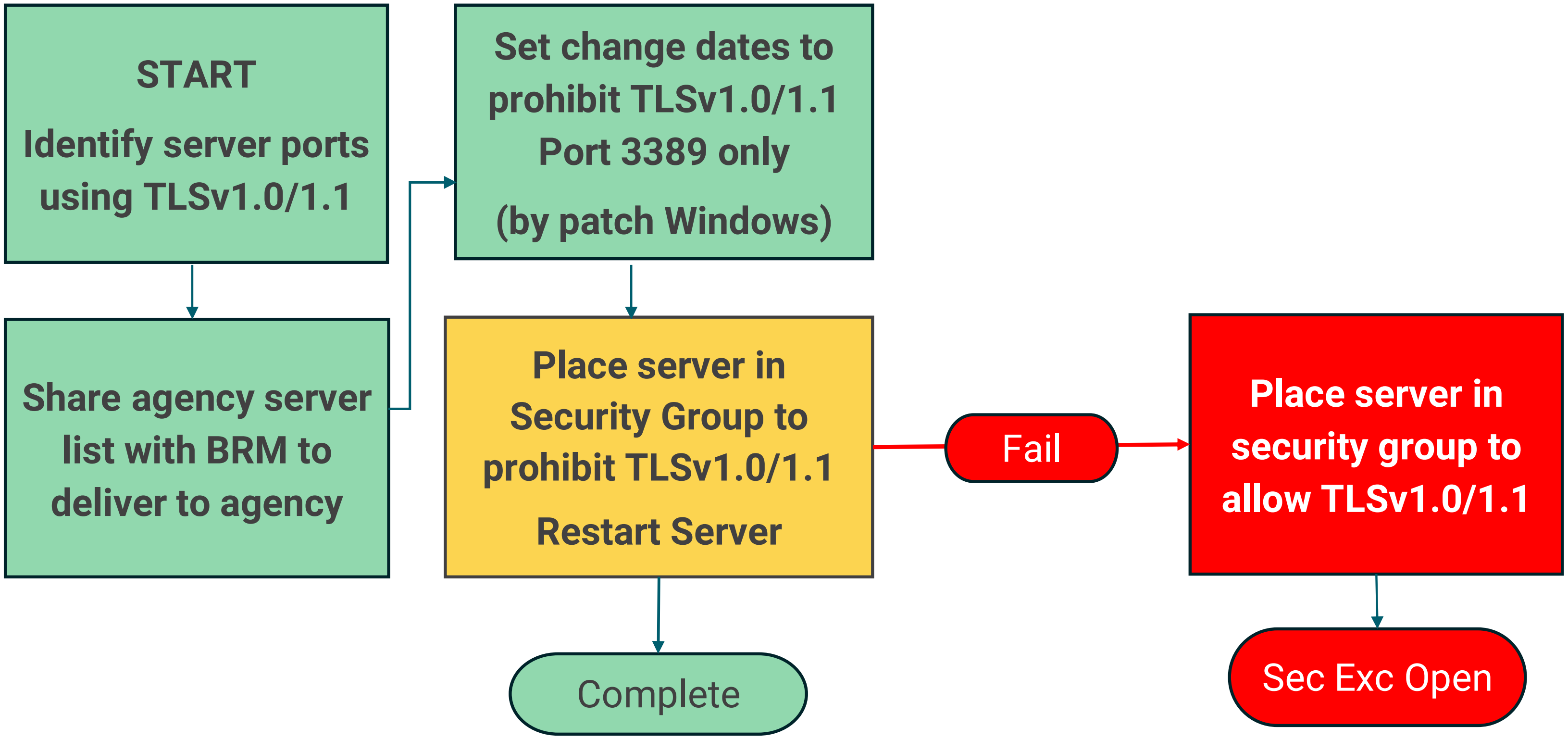
Remediation

1. Identify open ports: Identify any open TCP ports in your security groups or network access control lists (ACLs) that allow inbound traffic to port 3389 (RDP).
2. Restrict access: Restrict access to TCP port 3389 (RDP) by modifying the security group rules and network ACLs to allow inbound traffic only from trusted sources. This can be done by adding specific IP addresses or IP address ranges to the allowed list.
3. Implement additional security measures: Implement additional security measures such as two-factor authentication and encryption to strengthen the security of RDP connections.
4. Test and validate: Test your new security group rules and network ACLs to ensure that they are functioning as expected and that only authorized sources can access port 3389 (RDP).
5. Monitor and update: Regularly monitor your security group rules and network ACLs for changes and update them as needed to ensure that your systems are always protected against unauthorized access through TCP port 3389 (RDP).

How can agencies get ahead of the EOL encryption deprecation?

1. Determine if your agency-owned application(s) supports use of v1.2+
2. Check the operating system (OS) settings. If the OS security settings on a server have been changed to allow ‘any’ TLSv1.x, change those switches back to TLSv1.2+ only
3. If agency applications cannot support TLS1.2+, then submit a security exception(s) in Archer to identify the server name and agency application, along with the remediation actions required

Process to change RDP port to accept TLSv1.2/1.3 only



START

Identify server ports using TLSv1.0/1.1

Share agency server list with BRM to deliver to agency

Set change dates to prohibit TLSv1.0/1.1 Port 3389 only

(by patch Windows)

Place server in Security Group to prohibit TLSv1.0/1.1

Restart Server

Complete

Fail

Place server in security group to allow TLSv1.0/1.1

Sec Exc Open

Security groups (Windows)

This new group performs the registry update to disable TLSv1.0/1.1 and enforce use on Port 3389

0000-GP-C-Windows Server Disable TLS 1.0 - 1.1 Enable 1.2

This group allows the enablement and continued use of TLS1.0/1.1 on Port 3389

0000-GP-C-Windows Server Disable TLS 1.0 - 1.1 Re-enable

Next steps

Activities

- Set dates for the Port 3389 restriction (Windows-based servers only) – Planned
  - **June 16:** Patch window “A/B” – 194 servers – Successful
  - **June 23 – July 3:** Run and review a new Tenable report, assess and verify the security group change on June 16
  - **July 15:** Patch window “C” – 5 servers – Planned
  - **July 16:** Patch window “D” – 21 servers – Planned
  - **July 20:** Patch window “E” – 323 servers – Planned (production servers)
  - **July 22:** Patch window “X” – 1 server – Planned
  - **July 23:** Patch window “F” – 27 servers – Planned
  - **July 23 – Aug. 1:** Run and review a new Tenable report, assess and verify the security group change in the enterprise

Project closeout

Activities

- Based on Tenable scans, plan agency participation for remaining servers that either did not take the group policy objects (GPO) or will require additional testing on a per-server basis
- Work the GPO activation by Keystone Edge (KSE) Request
- Publish final report

Thank you to all the Agencies who have actively taken steps to remediate servers.

Questions?

Server Vulnerability Compliant Patching Schedule

SEC530 30-Day ‘High’ and ‘Critical’ Compliance

John C. Del Grosso

Agenda

- Patch process “Then and Now”
- Server patching process
- Typical three (3) month patching cycles
- Server patching window assignments
- Vulnerability strategies

Patching processes

- **Occurrence:** Done weekly, sometimes daily, depending on application ownership and VITA/supplier responsibility
- **Automation:** Most patching by Unisys is automated using the Ivanti Management System (Windows) and 'kron'/'yum' (Linux) with little manual intervention unless a problem or issue occurs
- **Reporting:** The Ivanti system reports the patch results, any issues or failures are investigated by the server, storage and data center (SSDC) patch team and rectified
- **Manual patching:** Used for applications or other situations where patches did not ‘take’

Primary differences from past to future patching cycles

	Past	Present
Occurrences	Patches occurred over a month (30-day period)	Patch cycles planned over a two-week period, with two patch cycles per month (aptly named Cycle 1 and Cycle 2)
Duration	Two-week patch checkout and test cycle before applying to production	One-week patch checkout and test cycle before applying to production
Change holds	Patch would be pushed to the next month	Patch would be pushed to the next patch cycle, **OR** a new temporary patching schedule is published
Security exceptions	Patches were generally applied within the 60 to 90-day time requirement - no need for exceptions	Agencies that push or delay patching beyond 30-day cycle must submit a security exception for the specific servers (in the case of agency-owned apps)

Patch calendar: 90-day outlook (June-July-Aug.)

Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday (CHG/Patch freeze by agency)
9	10 **Microsoft Patch Tuesday**	11	12 June primary election enterprise change freeze	13	14	15 DMV, DOA
16 June primary election enterprise change freeze	17	18	19 Juneteenth	20	21	22 DMV, DOA **Cycle 1: B-Pilot**
23	24	25	26	27	28	29 DMV, DOA **Cycle 1: E-Production**
30	**1 July** **Critical high**	2	3 July 4th weekend enterprise change freeze	4	5	6 DMV, DOA
7	8 **Microsoft Patch Tuesday**	9	10	11 **30 days**	12	13 DOA **Cycle 1: B-Pilot**
14	15	16	17	18	19	20 DOA **Cycle 1: E-Production**
21	22 **Critical high**	23	24	25	26	27 DOA **Cycle 2: B-Pilot**
28	29	30	31	**1 Aug**	2	3 **Cycle 2: E-Production**
4	5 **Microsoft Patch Tuesday**	6	7	8 **30 days**	9	10 **Cycle 1: B-Pilot**

VIRGINIA IT AGENCY

vita.virginia.gov

What has been the result of a two-cycle patch schedule?

- Difficult to assess after three (3) months (April/May/June)
- Technical difficulty with Avanti in May skewed the numbers where there was markedly more remediation in Cycle 2 than expected
- Numerous patch holds due to weather in Dec/Jan/Feb didn’t reflect a “normal’ patch cycle
- June patch holds for Juneteenth and Fourth of July so close together caused a shift in the patching cycle (cancelled Cycle 2 for June)
- Expect to have better and more reliable data after the July and August to assess fully

Updates in discussion

- The introduction of a two-cycle patch schedule has provided choices for agencies to manage resources throughout the month in support of patch and vulnerability management.
- Additional changes of process in consideration:
  - Release of the server list earlier in the week.
    - Currently (for Patch Window B & E) the list is released on Friday. The teams are **discussing release on Wednesday** to allow Agencies time to review and submit tickets to remove or adjust patching.
  - A unified patch schedule that considers servers that are managed by different suppliers (e.g. Unisys and NTT Data (Azure)).

Patch cycle management strategies

Start thinking – Vulnerability management vs. patch management

- **Vulnerability:** Manage the security patches by severity to meet the 30-day requirement
- **Patch:** Manage the non-security and low-security patching to meet the 90-day requirement
- Patches will always be released, but **less than 10%** are critical/high or CVSS 7.0 or higher
- Choose the cycles that an agency wants to spend the most resources to checkout and remediate

Suggested Patch cycle management checklist

- ❑ Review the upcoming patch list for severity score SV0
- ❑ Review the servers listed for participation
- ❑ Opt-out or -in of patch cycles that affect your vulnerability position

Slide 52

SV0 [@Delgrosso, John (VITA)] where can they find the score?

Vinoba, Susanna (VITA), 2025-06-24T15:30:45.146

Questions?

VIRGINIA IT AGENCY

vita.virginia.gov

Announcements

ISOAG July 9, 2025

International Travel

As traveling season approaches us, lets make sure we all understand how to comply with COV guidelines regarding devices.

Before your trip, be sure to check out the knowledge base article on the VCCC site if you are travelling internationally.

If you're unsure about any compliance requirements, don't hesitate to ask!

SPLUNK UPDATE July 2025

WE WANT YOUR LOGS:

VITA is working 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.

Top 5 Vulnerabilities

For the month of July, the Top 5 Key Vulnerabilities are:

- **Microsoft Windows Unquoted Service Path Enumeration**
- **Insecure Windows Service Permissions**
- **Microsoft XML Parser (MSXML) and XML Core Services Unsupported**
- **Palo Alto GlobalProtect Agent Privilege Escalation (CVE-2024-5915)**
- **SigPlus Pro ActiveX Control < 4.29 Multiple Vulnerabilities**

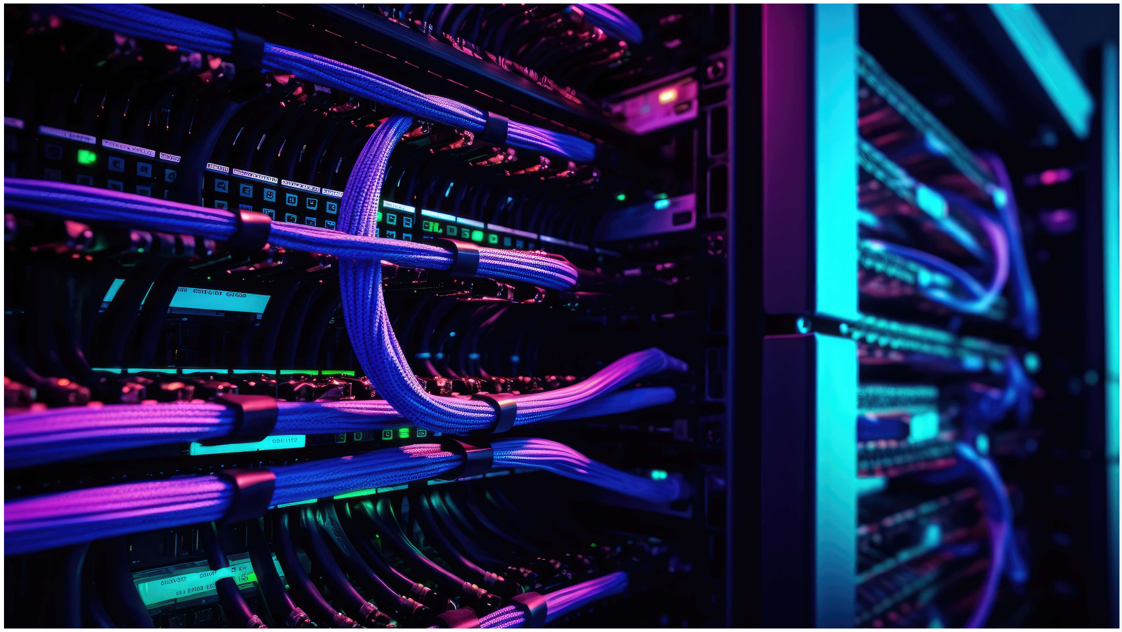
NOTE Check CSRM Connections for more detailed information

Upcoming Events

VIRGINIA
IT AGENCY
vita.virginia.gov

Governance Office Hours Announcement

Governance Office Hours launch recently – a dedicated space for Agency ISOs and teams to bring their questions, concerns, or ideas directly to the Governance Team.



What to Expect:

- **Open discussion place**
- **Governance Updates**
- **Q&A and support for your needs**

Next Session:
July 16th, 2025 | Microsoft Teams
[Click here to join the meeting]

Let's work together to strengthen governance across the Commonwealth!

Commonwealth of Virginia Information Security Conference 2025

ISC:25

Future-Proofing Cybersecurity: *Next-Gen Strategies*

August 14, 2025

Earn 5 CPE credits!

Register by July 25 to secure a printed name badge!

(Registrations after this date will require a handwritten badge)

[Security Conference | Virginia IT Agency](#)

[Registration page](#)

Service Tower SOC Report Review Sessions

The upcoming SOC review session is September 18, 2025, and will be held remotely.

Please register at the link below

To register for this meeting, please click on the link below:
https://covaconf.webex.com/weblink/register/r356265cb4b5d84cfa98903fb0adb74f2

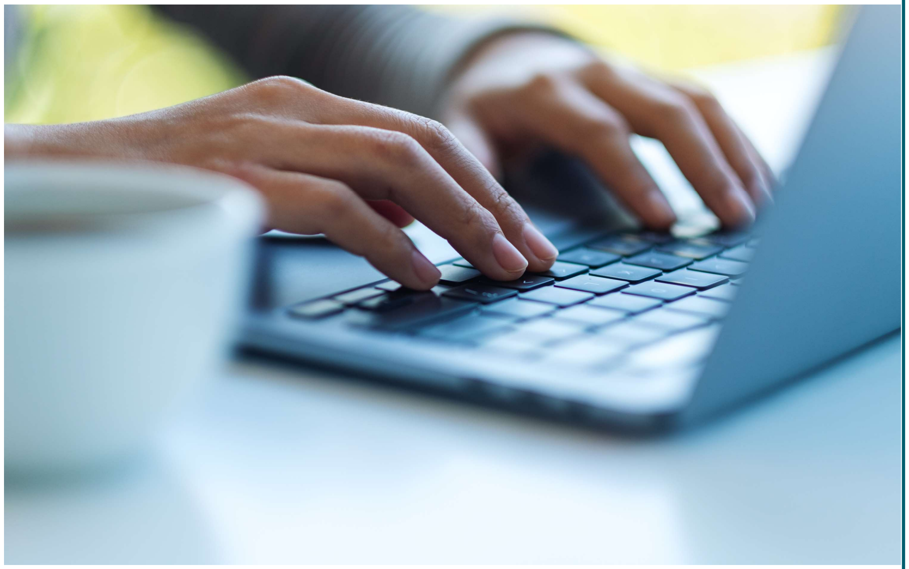
IS Orientation

The next IS Orientation is being held on September 24, 2025

- September 24, from 9am to 4pm, registration closes Sept 17th.
- It will be held in-person at the Boulders location:

7325 Beaufont Springs Drive, Richmond, VA 23225

- Visit Commonwealth IS Orientation to register!



MEETING ADJOURNED

VIRGINIA
IT AGENCY