VIRGINIA
IT AGENCY

Information Security Officer's Advisory Group

VIRGINIA IT AGENCY

Agenda	Presenter
Welcome/Opening Remarks	Kendra Burgess/ VITA
Impact of AI on information security practice and practitioners	Lionel Mew, Ph.D / University of Richmond
Cybersecurity Considerations During All-Hazards Incidents	Monroe Molesky / VDEM
Security Governance: Policies & Standards	Amy Braden / VITA
COV Tabletop Exercise 2025	Zach Wilton / SAIC
Announcements and Upcoming Events	Kendra Burgess/ VITA
Adjourn	

HOW ARTIFICIAL INTELLIGENCE IS TRANSFORMING CYBERSECURITY AS A PROFESSION

DR. LIONEL MEW

The Impact of AI on Information Security Practice and Practitioners

Executive Summary

The Transformation is Already Here

Artificial Intelligence has fundamentally altered the information security landscape, creating both unprecedented opportunities and complex challenges for cybersecurity professionals.

Key Impacts

- Threat actors leverage AI for sophisticated attacks
- Defensive capabilities enhanced through machine learning
- Professional skill requirements evolving rapidly
- New vulnerability categories emerging

Strategic Imperatives

- Upskill workforce in AI/ML technologies
- Integrate AI tools into security operations
- Develop AI governance frameworks
- Prepare for future AI-driven threats

Presentation Agenda

1. Historical Context

Pre-AI security landscape and limitations

2. Threat Evolution

AI-powered attack vectors and techniques

3. Defensive Capabilities

AI-enhanced security tools and processes

4. Skills Transformation

Evolving professional competencies

5. Operational Changes

Workflow automation and human roles

6. Future Outlook

Emerging trends and recommendations

Information Security: The Pre-AI Era

Traditional Security Approach

- **Signature-based detection:** Relying on known malware signatures
- **Rule-based systems:** Static security policies and configurations
- **Manual analysis:** Human-driven log review and incident response
- **Reactive posture:** Responding to threats after they occur
- **Perimeter-focused:** Network boundary security

Critical Limitations

- **Scalability issues:** Human analysts overwhelmed by data volume
- **False positive rates:** High noise-to-signal ratios
- **Detection lag:** Slow identification of novel threats
- **Resource constraints:** Limited 24/7 monitoring capabilities
- **Zero-day vulnerability:** Inability to detect unknown threats

The Challenge: Traditional security methods were struggling to keep pace with increasingly sophisticated and voluminous cyber threats, creating a clear need for technological augmentation.

The Evolution of Cyber Threats

AI-Enhanced Attack Vectors

Advanced Phishing

AI generates personalized, contextually relevant phishing emails that bypass traditional filters and human suspicion through sophisticated social engineering.

Deepfake Technology

Synthetic media creates convincing audio and video content for social engineering attacks, bypassing voice and video verification systems.

Automated Vulnerability Discovery

AI systems rapidly scan and identify zero-day vulnerabilities across networks, significantly reducing the time from discovery to exploitation.

Polymorphic Malware

Self-modifying malware that continuously evolves its code structure to evade signature-based detection while maintaining malicious functionality.

AI-Driven Reconnaissance

Automated intelligence gathering that analyzes social media, public records, and digital footprints to build comprehensive target profiles.

Adversarial Machine Learning

Attacks specifically designed to fool AI security systems by manipulating input data to cause misclassification and detection evasion.

Revolutionary Defensive Capabilities

Real-Time Threat Detection

Behavioral Analytics: AI monitors user and system behavior patterns to identify anomalies

Network Traffic Analysis: ML algorithms detect suspicious communication patterns

Endpoint Protection: AI-powered antivirus adapts to new threats in real-time

Threat Intelligence: Automated correlation of global threat indicators

Predictive Security

Risk Assessment: AI predicts potential attack vectors before exploitation

Vulnerability Prioritization: ML ranks vulnerabilities by actual risk level

Threat Hunting: Proactive search for advanced persistent threats

95%

Reduction in false positives with AI-driven security tools

200x

Faster threat detection compared to manual analysis

99.9%

Uptime for automated security monitoring systems

Professional Skills Transformation

Foundation Skills (Always Essential)

- Network security fundamentals
- Risk assessment methodologies
- Incident response procedures
- Compliance frameworks (SOX, HIPAA, GDPR)
- Security architecture principles

Emerging AI Competencies

- Machine learning concepts and algorithms
- Data science and statistical analysis
- AI model training and validation
- Algorithmic bias detection and mitigation
- Python/R programming for security analytics

Hybrid Integration Skills

- Human-AI collaboration strategies
- Adversarial AI and defensive techniques
- AI security governance and ethics
- Explainable AI for security decisions
- AI system security and hardening

Operational Workflow Evolution

Tasks Now Automated

- **Log Analysis:** AI processes millions of log entries in real-time
- **Initial Triage:** Automated classification of security incidents
- **Vulnerability Scanning:** Continuous automated network assessment
- **Compliance Monitoring:** Real-time policy violation detection
- **Threat Intelligence:** Automated feed processing and correlation
- **Basic Response:** Automated containment of routine threats

Enhanced Human Roles

- **Strategic Planning:** Long-term security architecture design
- **Complex Investigation:** Multi-stage attack analysis
- **AI System Management:** Tuning and optimizing ML models
- **Stakeholder Communication:** Translating technical risks to business impact
- **Threat Hunting:** Proactive search for advanced threats
- **Crisis Management:** Coordinating response to major incidents

Key Transformation: Security professionals have evolved from reactive monitors to proactive strategic leaders, with AI handling routine tasks while humans focus on complex decision-making and strategic planning.

AI-Specific Security Vulnerabilities

Model Poisoning

Attackers corrupt AI training data to manipulate model behavior, causing security systems to misclassify threats or ignore malicious activity.

Adversarial Attacks

Carefully crafted inputs designed to fool AI systems into making incorrect decisions, bypassing security controls through algorithmic manipulation.

Prompt Injection

Malicious prompts that manipulate AI language models to produce harmful outputs, bypass safety measures, or reveal sensitive information.

Model Extraction

Techniques to steal proprietary AI models through query-based attacks or reverse engineering, compromising intellectual property and security.

Data Poisoning

Injection of malicious data into AI training sets to create backdoors or degrade system performance over time.

AI Supply Chain Attacks

Compromise of AI development pipelines, pre-trained models, or AI-as-a-Service platforms to inject malicious functionality.

Regulatory and Compliance Evolution

Emerging AI Governance Requirements

New Compliance Areas

- **AI Impact Assessments:** Mandatory evaluation of AI system risks and societal impact
- **Algorithmic Transparency:** Requirements for explainable AI decisions in critical systems
- **Bias Testing:** Regular audits for discriminatory outcomes in AI applications
- **Data Governance:** Enhanced privacy protection for AI training data
- **AI Ethics Boards:** Governance structures for responsible AI deployment

Professional Implications

- **Cross-functional Collaboration:** Work with legal, ethics, and compliance teams
- **Documentation Requirements:** Comprehensive AI system audit trails
- **Continuous Monitoring:** Ongoing assessment of AI system performance and bias
- **Incident Response:** AI-specific breach notification procedures
- **Training Requirements:** Ongoing education on AI governance and ethics

Strategic Importance: Security professionals are now key stakeholders in AI governance, requiring deep understanding of both technical and ethical implications of AI implementations.

Career Transformation and Opportunities

Emerging Specialized Roles

- **AI Security Architect:** Design secure AI systems and infrastructure
- **ML Security Engineer:** Implement and maintain AI-powered security tools
- **AI Threat Intelligence Analyst:** Analyze AI-driven attack patterns
- **Adversarial AI Specialist:** Develop defenses against AI-powered attacks
- **AI Compliance Officer:** Ensure AI systems meet regulatory requirements
- **AI Ethics and Governance Consultant:** Guide responsible AI implementation

Evolved Traditional Roles

- **Security Analyst** → AI-Augmented Threat Hunter
- **SOC Manager** → AI Operations Center Director
- **CISO** → AI-Aware Security Executive
- **Incident Responder** → AI-Assisted Investigation Lead
- **Compliance Officer** → AI Governance Specialist
- **Security Architect** → AI-Integrated Security Designer

78%

Increase in demand for AI-skilled security professionals (2024-2025)

Implementation Challenges and Solutions

Major Challenges

- **Skills Gap:** Shortage of AI-literate security professionals
- **Integration Complexity:** Difficulty incorporating AI into existing security infrastructure
- **False Positive Management:** Balancing sensitivity with accuracy in AI detection
- **Explainability:** Understanding how AI systems make security decisions
- **Cost and ROI:** Justifying AI investment with measurable returns
- **Data Quality:** Ensuring clean, representative training data
- **Vendor Selection:** Choosing appropriate AI security solutions

Strategic Solutions

- **Phased Implementation:** Gradual AI adoption with pilot programs
- **Continuous Learning:** Ongoing training and certification programs
- **Human-AI Collaboration:** Frameworks for optimal human-machine interaction
- **Explainable AI:** Adoption of interpretable machine learning models
- **Threat Intelligence Sharing:** Collaborative defense through shared AI insights
- **Cross-functional Teams:** Integration of security, data science, and business units
- **Vendor Partnerships:** Strategic relationships with AI security providers

Success Factor: Organizations that invest in comprehensive change management, including people, process, and technology transformation, achieve the most successful AI security implementations.

Future of AI in Information Security

Emerging Trends and Technologies

Autonomous Security Operations

Self-managing security systems that automatically detect, investigate, and respond to threats with minimal human intervention.

Quantum-Resistant AI Security

AI systems designed to withstand quantum computing attacks while leveraging quantum capabilities for enhanced security.

Zero Trust AI Architecture

AI-powered systems that continuously verify and validate all security decisions and access requests in real-time.

Federated AI Security

Collaborative AI models that share threat intelligence across organizations while preserving data privacy.

AI-Generated Security Policies

Dynamic policy creation and adjustment based on real-time threat landscape analysis and organizational risk tolerance.

Cognitive Security Operations

AI systems that can reason, learn, and adapt to new threats using advanced cognitive computing capabilities.

Prediction: By 2030, AI will be seamlessly integrated into every aspect of information security, fundamentally changing how we conceptualize and implement cyber defense strategies.

Maintaining Practitioner Relevance

Immediate Actions (0-6 months)

- Complete online ML fundamentals courses
- Experiment with AI security tools in lab environments
- Join AI security professional communities
- Conduct AI vulnerability assessments
- Attend AI security webinars and conferences

Short-term Goals (6-18 months)

- Obtain AI/ML security certifications
- Implement AI-augmented security workflows
- Develop organizational AI governance frameworks
- Build cross-functional AI security teams
- Pilot AI security tools in production

Medium-term Strategy (1-3 years)

- Specialize in specific AI security domains
- Lead AI transformation initiatives
- Contribute to AI security research and standards
- Mentor emerging AI security professionals
- Develop AI security thought leadership

Long-term Vision (3+ years)

- Become recognized AI security expert
- Shape industry AI security standards
- Publish AI security research and best practices
- Consult on enterprise AI security strategies
- Influence AI security policy and regulation

Key Takeaways and Action Items

Critical Success Factors

For Individuals

- Embrace continuous learning in AI/ML technologies
- Develop both technical and strategic AI competencies
- Focus on human-AI collaboration skills
- Stay current with emerging AI threat vectors
- Build cross-functional relationships

For Organizations

- Invest in comprehensive AI security training
- Implement phased AI integration strategies
- Establish AI governance and ethics frameworks
- Foster culture of innovation and experimentation
- Build strategic vendor partnerships

The Bottom Line

AI is not replacing security professionals—it's amplifying their capabilities and creating new opportunities for those who adapt and evolve with the technology

Thank you!

Lionel Mew, Ph.D.

Assistant Professor and Chair, Information Systems

School of Professional and Continuing Studies

University of Richmond

lmew@richmond.edu

Office: (804) 289-8944

Cell/text: (804) 384-7913

Virginia Department of Emergency Management

Cybersecurity Considerations During All-Hazards Incidents

Monroe J. Molesky
Cyber Resilience Program Manager

September 3, 2025 – ISOAG Meeting

About VDEM

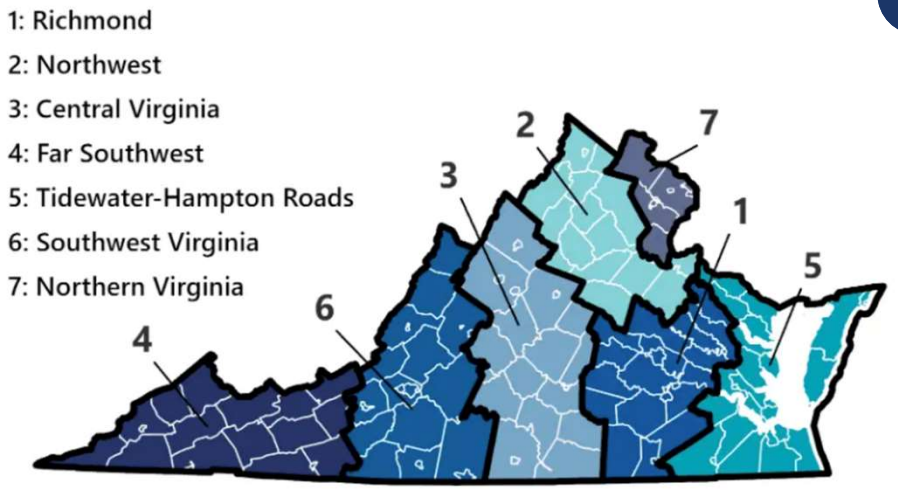
- **Mission:** To save lives…by coordinating a whole of Commonwealth approach to any complex event or disaster including, but not limited to, any natural, man-made, acts of terrorism, or cyber-related incident or event.

- **Responsibilities include:**
  - Develop/Maintain Statewide Emergency Operations Plans
  - Coordinate Multiagency/Statewide Responses
  - Deliver Training and Exercise Programs
  - Support Local 911 Public Safety Answering Points
  - Manage Grants as the State Grants Authority

Start Local, End Local

- VDEM maintains seven regional offices each with:
  - Chief Regional Coordinator
  - All-Hazards Planner
  - Disaster Response and Recovery Officer
  - Recovery and Mitigation Specialist
  - Hazardous Materials Officer

~25% of VDEM Staff are Located in Regions



Virginia Emergency Support Team

17 Emergency Support Functions (ESF), sourced from:

- More than 250 members
- State Agencies
- Private Sector
- Non-Governmental Organizations (NGO's)

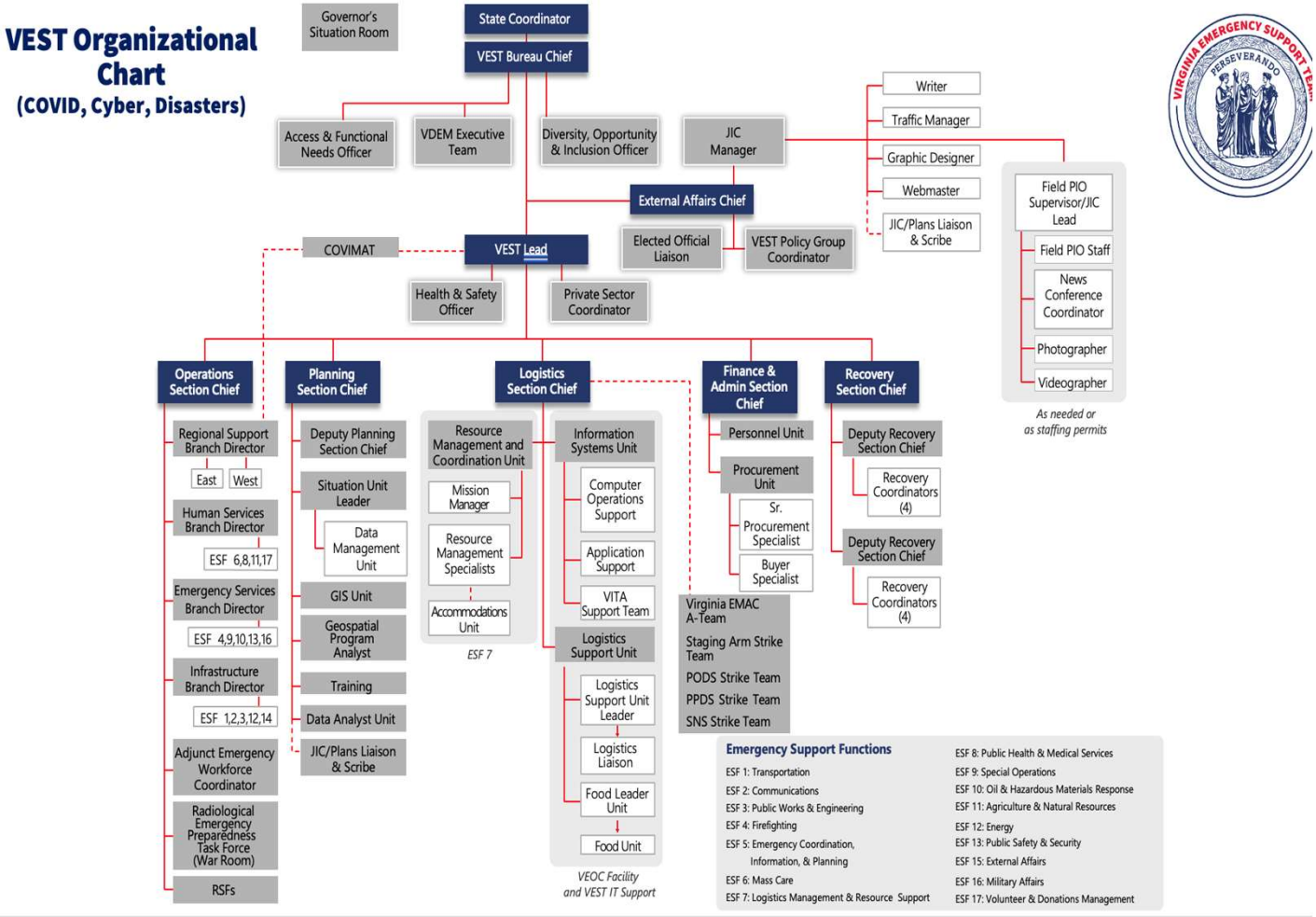
Outside the Commonwealth assistance, sourced from:

- Federal Emergency Management Agency (FEMA)
- Emergency Management Assistance Compact (EMAC)
- Department of Defense (DOD)
- Cybersecurity and Infrastructure Security Agency (CISA)

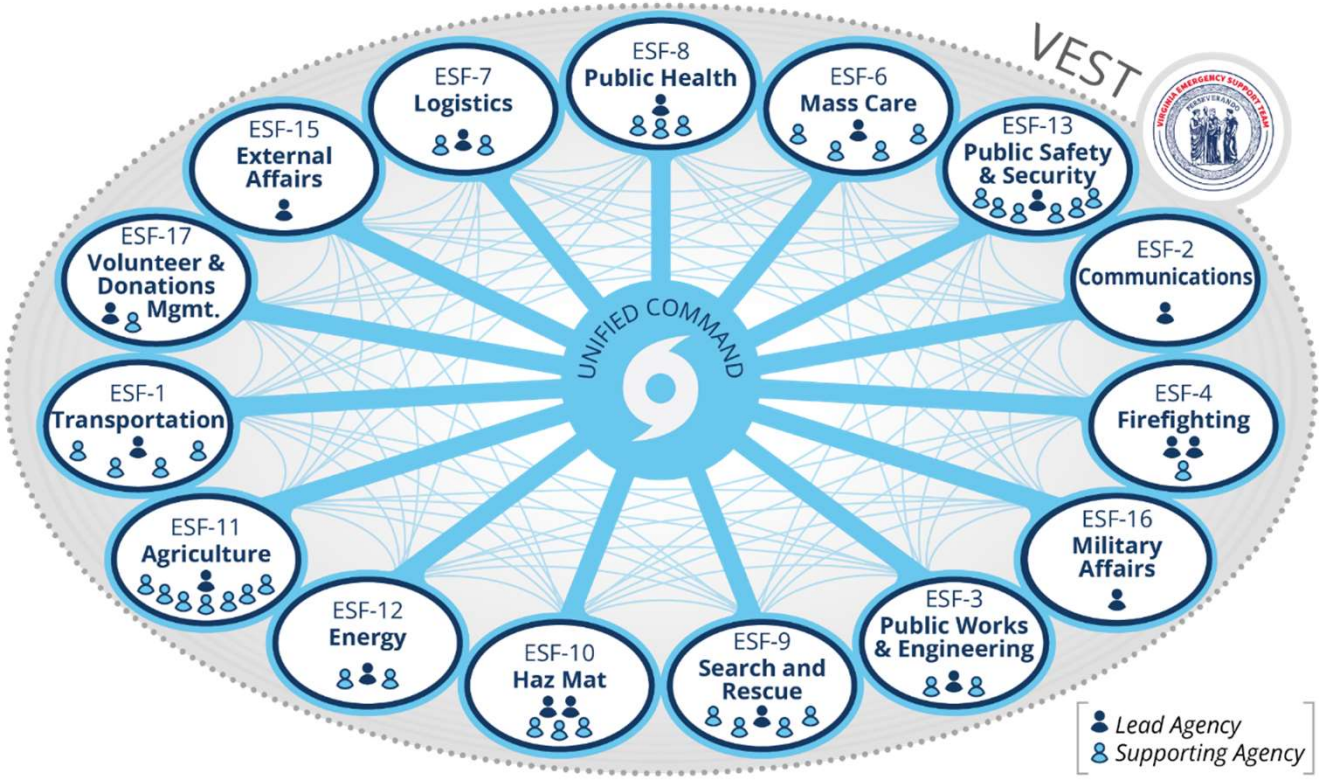
Commonwealth of Virginia Emergency Operations Plan (COVEOP) describes how Virginia will respond and recover from all threats

- Title 44, Code of Virginia and Executive Order (EO) 41

VEST Organizational Chart
(COVID, Cyber, Disasters)



Virginia Emergency Support Team



Cyber and the All-Hazards Landscape in the Commonwealth

VDEM Cyber Resilience Program

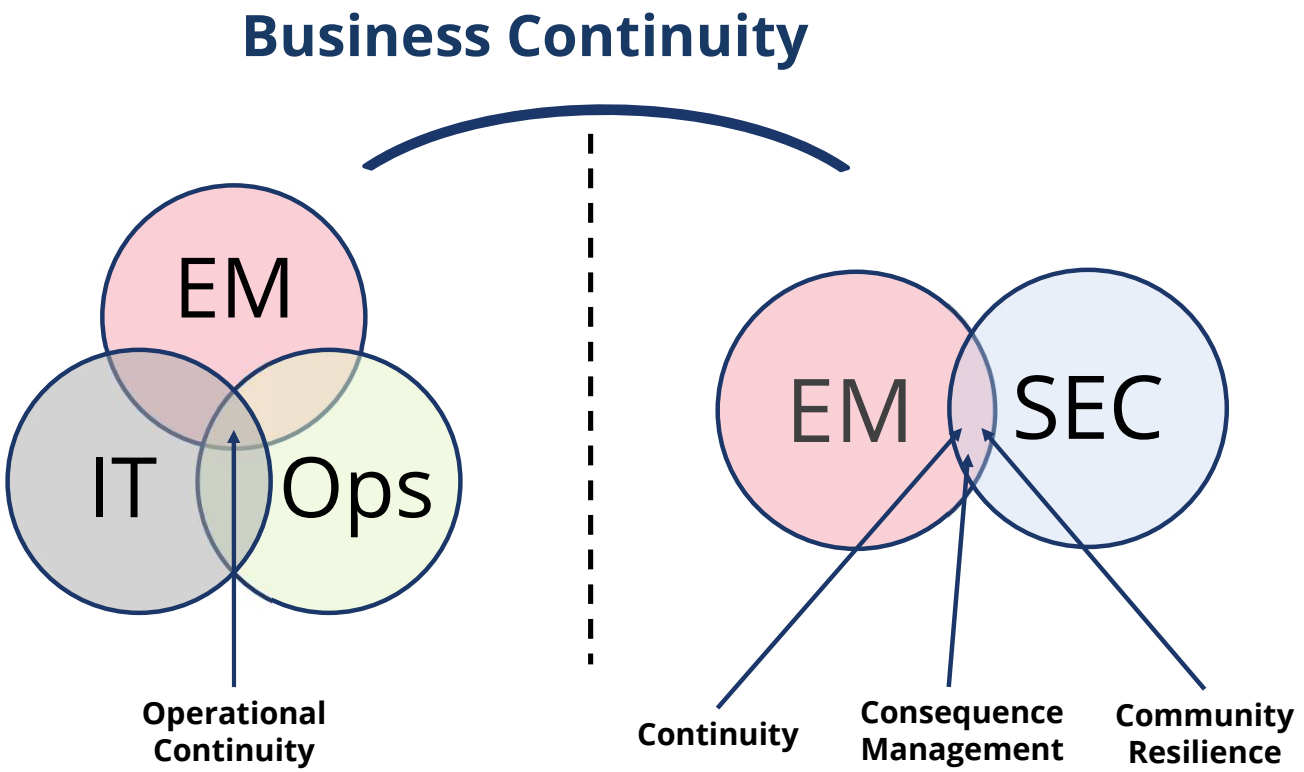
Mission: Bring together public and private sector partners to advance the resiliency of stakeholders across the Commonwealth of Virginia to cybersecurity threats.

- **Focus Areas:**
  - **O**utreach
  - **P**artnerships
  - **T**raining, Exercises, & Planning
  - **R**egional Support
  - **I**ncident Coordination

Whole-of-Commonwealth Cyber Approach

- Shared understanding of community needs and capabilities
- Establishment of relationships that facilitate more effective prevention, protection, mitigation, response, and recovery activities
- Greater integration of existing resources from local to federal level
- Empowerment of innovation and localized solutions

Emergency Management & Cyber



Cyber Threats During All-Hazards Incidents

All-hazards incidents do not always occur singularly, but several incidents and events can occur simultaneously including cyber.

Cyber threat actors increasing seek opportunities to exploit vulnerabilities during occurring non-cyber incidents:

All-Hazards Threats

Examples:

- Chemical Emergencies
- Cybersecurity
- Earthquake and Landslides
- Flooding
- Health Threats
- Hurricanes
- Nuclear Safety
- Terrorism
- Tornados

Emergency Management Cycle

All-Hazard Threats: Hurricane Scenario

Annual Atlantic Hurricane Season: June 1st to November 30th

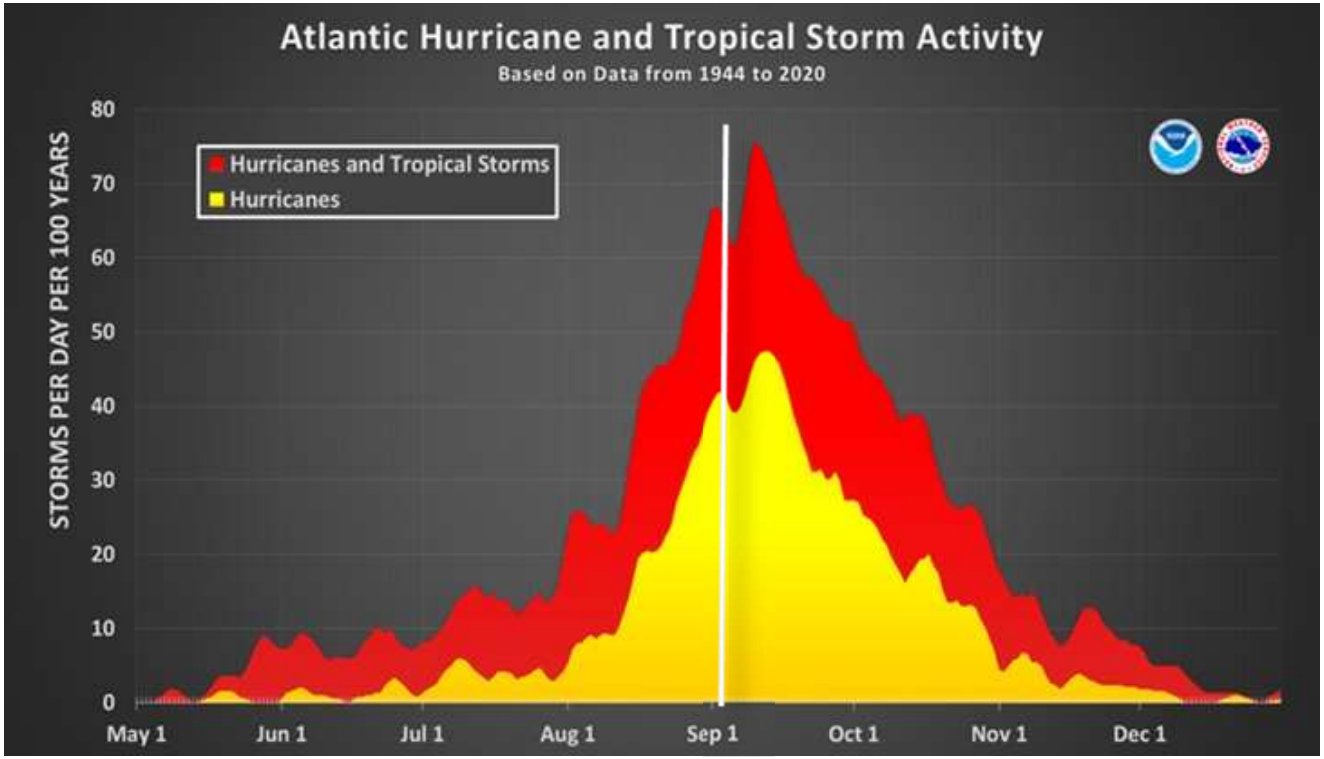
HURRICANES IN VIRGINIA

Hurricane Camille Aug. 19-20, 1969	Dropped 27 inches of rain on Nelson County in eight hours, resulting in 153 fatalities from flash floods and mudslides.
Tropical Storm Agnes June 21, 1972	Dropped 16 inches of rain on Fairfax County. At the height of the flooding, more than 600 miles of highways were submerged across the state.
Hurricane Fran Sept. 5-6, 1996	Dropped 8 to 16 inches of rain over the mountains and the Shenandoah Valley; in one hour some areas saw 3.5 inches of rain.
Tropical Storm Isabel Sept. 18, 2003	Dropped 20 inches of rain in Sherando, Va. Turned 100 Virginia localities into disaster areas and the storm killed 32 people. 80% of the state's population was without power.
Hurricane Matthew Oct. 8-9, 2016	Dropped more than a foot of rain in southeast portions of Virginia; rainfall and moderate tidal flooding led to severe flooding and more than 260,000 customers were without power.

Hurricane Helene – September 2024

Aftermath of Hurricane Helene in Washington County, VA and Grayson County, VA
(Pictures Taken By VDEM)

Historical Hurricane Activity



(Courtesy of VDEM Hurricane Program)

Question:

What may ISOs consider during an all-hazards incident, such as a hurricane, impacting the Commonwealth?

Cybersecurity Considerations

Monitor the Landscape

Internal Cyber

- CISA “Shields Up” campaign approach
- Emphasis on monitoring and log review for systems that are public facing, critical for continuity, or essential for public safety in an incident.

External Cyber

- Engage Virginia Fusion Center that integrates both cyber and other intelligence during incidents.

Incident/Emergency Management

- Monitor status of the Virginia Emergency Support Team/Virginia Emergency Operations Center (vaemergency.gov).
- Engage your agency emergency manager (if applicable)

Support Personnel

Educate personnel to identify phishing and scams during incidents.

- Develop and execute all-hazards related security education throughout year.
- Send reminders/information during specific incidents.

Plan for identification and authentication contingencies.

- Communicate alternatives for if a COV issued device/key used for MFA is lost.
- Plan for new or escalated accounts and privileges during surge staffing.

Consider impact of previously scheduled downtime, updates, or other changes.

Physical Security with Cyber

Collaborate with facility personnel to plan for security of IT infrastructure at locations impacted during incidents.

- Physical security with transition to telework during incidents.

Support education on physical-cybersecurity best practices during incidents.

- Reminders on “tailgating” especially with potential new personnel supporting activities.
- Securing physical devices during activities in the field.

Communication

Amplify cyber information during all-hazards incidents to your stakeholders and through existing channels.

Coordinate public incident-related communications with the incident support structure, where appropriate (e.g., VEST Joint Information Center)

Share timely cyber risk and cyber incident information.

- Even during ongoing non-cyber incidents, additional resources to support cyber incident responses are coordinated.

Questions?

Monroe J. Molesky, MPH, MBA
Cyber Resilience Program Manager
monroe.molesky@vdem.virginia.gov | (804) 866-7779

cyber@vdem.virginia.gov

VIRGINIA IT AGENCY

CSRM Security Policies and Standards

Information Security Office Advisory Group (ISOAG)

Amy Braden
Director, IT Security Governance & Compliance

September 3, 2025

Authority and scope

Virginia Code § 2.2-2009 creates a scope of cybersecurity governance that is broader than VITA's core executive branch agencies: "executive, legislative, and judicial branches and independent agencies"

- But does NOT apply throughout state government, with exclusions for higher ed and authorities
- Much less visibility, from both technical and compliance perspectives, outside the executive branch

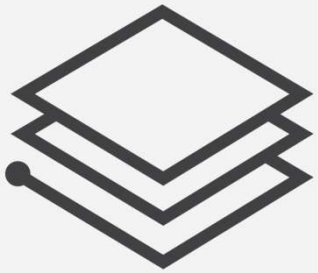
Primary objectives are to assess security risk, determine appropriate security measures and perform security audits of government electronic information.

Key policies and standards

In 2023, Cybersecurity and Risk Management (CSRM) published SEC530 a consolidation of SEC501 and SEC525 and update to the NIST 800-53

8 key policies and standards addressing cybersecurity:

- Information Security Policy (SEC519)
- Information Security Standard (SEC530)
- IT Risk Management Standard (SEC520)
- IT Security Audit Standard (SEC502)
- Security Awareness Training Standard (SEC527)
- IT Standard Use of Non-Commonwealth Computing Devices to Telework (SEC511)
- Removal of Commonwealth Data from Electronic Media Standard (SEC514)
- Data Classification Standard (SEC540)*



Key deliverable guidelines and templates are available on the VITA website.

The edit and review process

- Document revision process involves collaboration and review with agency ISOs informally and formally.
- Documents are posted to ORCA* for a minimum of 30 days for non-administrative changes. If unable comply by the effective date, agencies may submit a security exception outlining that includes a plan to satisfy requirements.

CSRM shares regular updates in monthly forums such as ISOAG and ISO Council

*(*VITA's Online Review and Comment Application (ORCA) requires registration but is available to persons outside the executive branch, and even those outside state government entirely.)*

How’s it working?

Policy and standards provide Commonwealth flexibility

Policy and standard language is intentionally technology agnostic and non-prescriptive. Agency defined controls are available to accommodate agency needs.

For example, SEC530 has 244 agency defined controls. Applying broad language may be a challenge for some agencies.

Alignment with federal standards (e.g., NIST 800-53), ensures Commonwealth policies and standards meet needs of agencies with additional requirements and meets industry standards. This baseline makes it easier to assess security amid a variety of organizations.

- Federal compliance will streamline Commonwealth compliance too (e.g., FedRAMP).
- But strict federal alignment may appear more restrictive and overburdensome and not necessarily applicable at the state level.

Opportunity for improvements

- Resources permitting, CSRM could provide more standards and guidelines to meet specific needs.
- Be more prescriptive on how to meet standards.
- Provide more training to agencies on how they can leverage current policies and standards to meet their needs.
- Better agency and customer engagement as we need robust input.

Thank you

COV TABLETOP EXERCISE 2025

September ISOAG

Name: Zachary Wilton
Date: 9/03/25

TABLE OF CONTENTS/ AGENDA

- Overview
- Expected Outcomes
- Event Information

SAIC

OVERVIEW

The COV Annual Tabletop Exercise is an unclassified, adaptable exercise developed by the MSI/MSS for the Commonwealth of Virginia. The main purpose is to evaluate performance of the multisupplier model, promote dialogue around opportunities for continuous improvement, and identify recommendations for improvement for the COV Cybersecurity Incident Response process.

EXPECTED OUTCOMES

- Expected outcome from this event is to conduct a tabletop event where coordination of multiple Suppliers and Service Delivery ensures COV information systems will successfully operate in support of the exercise scenario, and when the managed environment is under attack.

  - Demonstrate successful coordination of multiple Supplier Service Delivery
  - Ensure COV information systems will successfully operate in support of the exercise scenario
  - Enhance awareness, readiness and coordination
  - Test capability to determine operational impacts of a cyberattack
  - Test participant's exercise playbooks, incident analysis, incident response plans and procedures, and incident reporting
  - Demonstrate compliance with MSI Security Incident Management Process SMM 4.1.5.7 and VITA Playbooks
  - Identify Enterprise-wide opportunities for improvement
  - Further integration of multi sourcing program between MSI, VITA-CSRM, Service Towers, and the Agencies

EVENT INFORMATION

- When:
  - Exercise: 10/28/2025 (Tuesday)
  - After-Action Review: 10/29/2025 (Wednesday)
- Who:
  - Hosted by: MSI SIRT team (SAIC), MSS SOC (ATOS), and VITA CSRM
  - Participants: IT Security Professionals from any/all Agencies and Service Towers part of the VITA Program
- Where:
  - Virtual only event: A link will be provided at a later date!

EVENT INFORMATION

- How to join:
  - Send an email to MSI-Security-Operations@saic.com stating that your agency/tower would like to participate in this year's event!
    - Please include the names and emails of the specific people that would like to participate from your agency/STS
    - RSVP Cut-Off: Oct 17th 2025

ANY QUESTIONS?

SAIC

Announcements

ISOAG September 2025

Acunetix Survey extended

- **Survey Name:** Acunetix 360 Customer Satisfaction Survey
- **Survey Link:** https://forms.office.com/g/K8PbAKrcC5
- **Available From:** August 7, 2025 through **September 9, 2025**
- **Why should ISOs do it?** It'll help us spot any gaps and see how the product is performing, so we can make it even better.

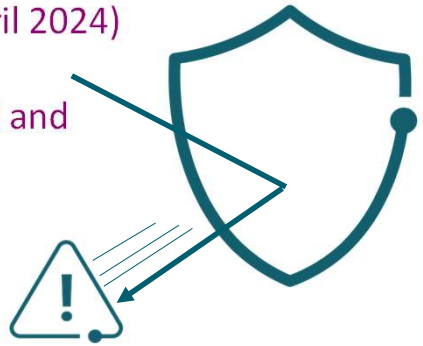
WE WANT YOUR LOGS:

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 September, the Top 5 Key Vulnerabilities are:

- Firefox < 141.0
- Zoom Workplace < 6.3.10 Vulnerability (ZSB-25030)
- Google Chrome < 138.0.7204.168 Multiple Vulnerabilities
- Security Updates for Microsoft SQL Server ODBC Driver (April, June, October 2023 and April 2024)
- Security Updates for Microsoft SQL Server OLE DB Driver (April June & October 2023, April and July 2024)



NOTE Check CSRM Connections for more detailed information

Upcoming Events

VIRGINIA
IT AGENCY
vita.virginia.gov

The October 1, 2025 ISOAG Meeting will be In-Person (and virtual)

Location: Reynolds Community College

Time: 1-4 pm

Please remember that in-person attendance is mandatory for primary, in-scope ISOs to maintain credentials. If one is unable to attend, you must let CSRM know and email the name of the designated person to come in your place by September 17.

Registration: In-person

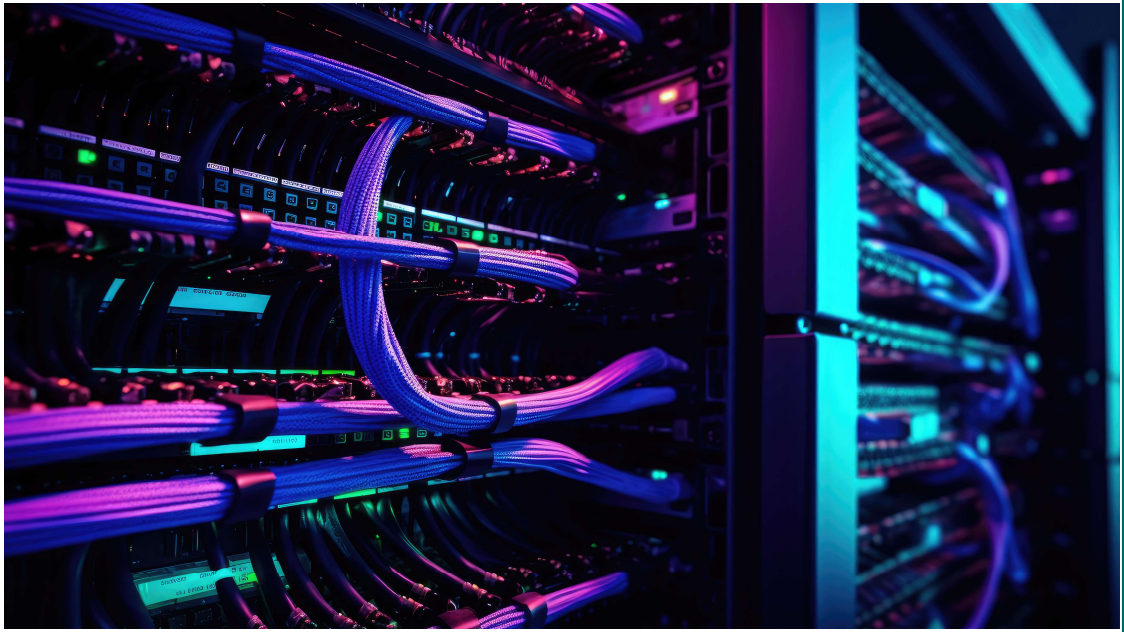
Virtual

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:
September 10, 2025 | Microsoft Teams
[Click here to join the meeting]

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

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

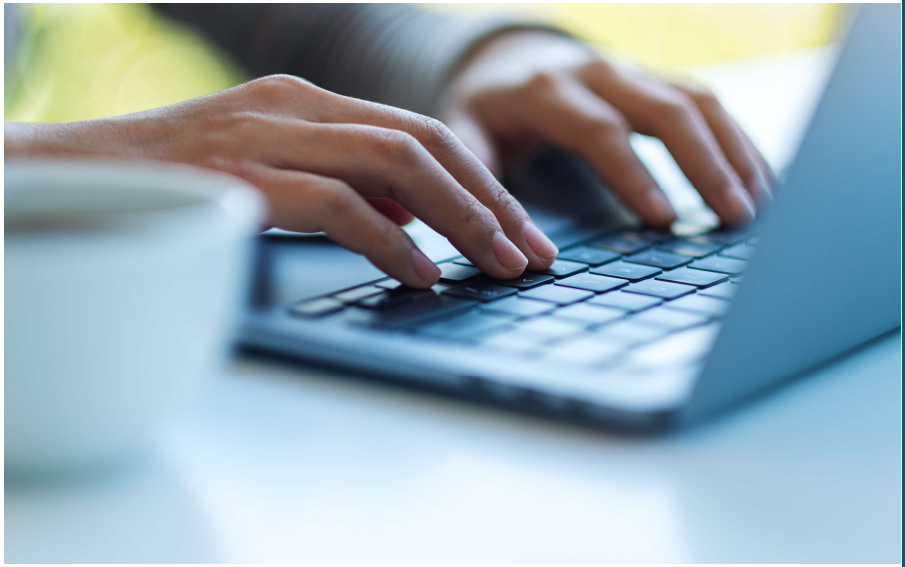
IS Orientation

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!



VASCAN

Registration is now open!

VASCAN

October 13 – October 14, 2025

Old Dominion University
Webb University Center
1301 W 49th St, Norfolk, VA 23529

MEETING ADJOURNED

VIRGINIA
IT AGENCY

VIRGINIA
IT AGENCY

Welcome to the Sept. 3, 2025 ISOAG Meeting

Information Security Officer's Advisory Group

WELCOME TO THE Sept. 3, 2025 ISOAG MEETING

VIRGINIA IT AGENCY

Information Security Officer's Advisory Group