Virginia Cybersecurity Planning Committee
July 15, 2026 – 10:00 a.m.
7235 Beaufont Springs Dr, Mary Jackson Boardroom,
Richmond, VA, 23225

Call to Order

A meeting of the Virginia Cybersecurity Planning Committee was called to order at 10:06am. Mr. Watson welcomed the members.

Presiding

Michael Watson, Committee Chair, Chief Information Officer, Virginia IT Agency

Members Present

Timothy Wyatt, Committee Vice Chair, Director of Information Technology, County of York
Troy Adkins, Broadband Infrastructure Program Manager, Chickahominy Indian Tribe
Diane Carnohan, Chief Information Security Officer, Virginia Department of Education
Robbie Coates, Director, Grant Management and Recovery, Virginia Department of Emergency Management
Brenna R. Doherty, Chief Information Security Officer, Department of Legislative Automated Systems
Charles Huntley, Director of Technology, County of Essex
Derek Kestner, Information Security Officer, Supreme Court of Virginia
Brandon Smith, Chief Information Officer, Department of Elections

Members Attending Virtually

Charles DeKeyser, Major, Virginia Army National Guard
Chris Mowry, Chief Information Technology Officer, Virginia State Police
Beth Burgin Waller, Chair, Cybersecurity and Data Privacy Practice, Woods Rogers Vandeventer Black

Members Not Present

Uma Marques, Information Technology Director, Roanoke County Government

Staff Present

April Gauldin, Legal & Legislative Services Coordinator, Virginia IT Agency
Mary Fain, Director of Information Security Programs, Virginia IT Agency
Janet Logan, Project Manager, Virginia IT Agency
Jaime Hoyle, Director of Legal and Legislative Services, Virginia IT Agency
Rebecca Askew, Policy and Governmental Affairs Manager, Virginia IT Agency
Ephfrom Walker, Legal Compliance and Policy Specialist, Virginia IT Agency
Jennifer Guild, Assistant Director of Communications, Virginia IT Agency
Advait Kulkarni, Junior Associate, Virginia IT Agency
Angevin White, Junior Associate, Virginia IT Agency

Review of Agenda

Mr. Kulkarni provided an overview of the agenda.

Approval of Minutes

The May 20 meeting minutes were displayed on the screen. Upon a motion by Mr. Wyatt and duly seconded by Mr. Smith, the committee unanimously voted to approve the May 20 meeting minutes.

Finances

Ms. Fain presented the financial update. There are no significant changes from the last meeting. The remaining allocations were discussed. The committee previously voted to authorize between $10.6 million (prioritized) up to $15.8 million. The program is currently at $8.7 million (estimated) between known licensing costs and projected implementation and maintenance costs. We anticipate needing up to the full $15 million to complete licensing and contingency for implementation and maintenance for all elements before getting to firewalls. There is an additional $2 million available for year 3 that is available to be allocated as well as year 4 funds, that do not have a project tied to it yet.

Phase 2 Project Update

Ms. Logan delivered an extensive update on the status of Phase 2 projects. There are currently still three areas in flight: Firewalls, the second round of Endpoint Detection Response (EDR), and the second round of Vulnerability Management. Application activity continues across all three, with firewalls having 66 applications submitted and 26 completed with full materials, vulnerability management with 25 applications, and EDR with 23 applications. The application window runs through July 17, with a commitment to expedite review and connect approved localities to vendors as quickly as possible. Phase 2 deployment and maintenance windows have been formally extended to October 31, with final project closure targeted for November. Asset and data inventory efforts are proceeding in parallel, with substantial progress reported. With asset inventory, a majority of participating localities have achieved greater than or equal to 70% completion. For data inventory, nearly all participating localities are approaching 70% completion. For Secure Remote Network Access (SRNA), the consent agreements received have reached about 65%. Ms. Logan highlighted that detailed planning for asset and data inventories may extend up to six months, depending on complexity across environments. To reduce operational disruptions, Phase 2 deployments are being strategically staggered, ensuring no single locality experiences excessive blackout periods. Chair Watson reported ongoing selection and negation for the Locality Security Operations Center (SOC) contract. Until the SOC is fully stood up, CrowdStrike Falcon Complete will serve as an interim monitoring capability for up to one year. This ensures continuity of endpoint threat detection across participating localities. An internal audit concluded in June covering all Phase 2 applications. Each locality received a customized summary assessing accuracy, completeness, and compliance. Staff reviewed 141 application folders, narrowing outstanding issues to fewer than ten as of the meeting date. Chair Watson expressed optimism that Phase 2 would reach full operational closure before year-end, enabling the committee to pivot more fully into Phase 3.

Phase 3 Follow Up

Ms. Fain reviewed the previous information received and discussed from Phase 3 surveys, including the strong response rate from localities, higher education, regional authorities, and tribal entities. The key themes were significant interest in workforce development and patch management. There was a clear preference for on-demand, self-paced training supported by virtual or hybrid modalities. There is a broad need for tool-specific content, alongside general framework and best practice guidance. Respondents also expressed operational constraints, with most organizations requiring 6-12 months of lead time to budget the training. Also, rural and smaller localities face greater staffing limitations, often able to release only one to three people at a time. Drawing from surveys and adult learning research, the committee explored a flexible skills-based model informed by a formal baseline assessment. Central elements include a skills assessment, with those scoring less than 50% confidence being strong candidates for training. Also, modality matching with training formats aligned

with locality preference (self-paced, virtual instruction, regional workshops, hands-on labs, and tool specific models). The use of outcome measurement in the form of the Kirkpatrick evaluation method (reaction, learning, behavior, results) will be supported by post training reassessments. Committee members raised thoughtful questions to be considered. Should certain training areas be mandatory, such as baseline cyber fundamentals? How do we integrate emerging technologies like AI-based security and deepfake identification? Can we ensure that localities receive concise updates, such as one-page survey summaries or program impact sheets?
Ms. Fain moved on to Patch Management program design. The survey results revealed inconsistent and frequently ad-hoc patching across Virginia localities. Respondents noted that they needed practical tools to close gaps in patching, clear Standard Operating Procedures (SOPs) to ensure long-term sustainment, and remediation support for initial catch up. The patch management model under consideration contains three areas. For patch management tool deployment, there will be a preference for tools already on statewide contract, cross-platform, and integrated with existing vulnerability management suites. For SOP development assistance, contracted resources will help localities tailor SOPs to their environments. For catch up remediation, supplemental help for entities significantly behind on patch cycles will be provided. Committee members debated the role of risk prioritization, support for end-of-life systems, and balancing centralized procurement with locality flexibility.
Chair Watson reopened discussion on funding allocations, reminding the committee that year 3 retains nearly $10 million for further program development and decisions regarding distribution among training, patch management, firewalls, and emerging needs must be finalized before upcoming budget cycles. Mr. Smith emphasized that any Phase 4 or capstone activities must be completed by July/August 2027 to align with legislative cycles.

Post Federal Grant Planning

Chair Watson noted that federal grant support is expected to conclude in 12-18 months. Early conversations the Joint Committee on Technology and Science (JCOTS) indicate interest in sustaining and expanding successful elements of the program. The Chair asked the committee to begin considering whether current governance should transition toward an ISAC model, how to capture and communicate statewide cybersecurity maturity gains, and what future committees/structures/focus areas should look like beyond 2027.

Public Comment Period

There were no public comments.

Other Business

Chair Watson opened the floor for other business. It was discussed that all committee members' terms expire in October. The Chair and Ms. Gauldin assured the members that it is being worked on and that mechanisms are in place to have the members continue their work on the committee. Chair Watson also encouraged members to follow updates and attend the Information Security Conference (ISC).

Ms. Gauldin discussed travel forms. Chair Watson cancelled the next meeting in August and Ms. Gauldin noted that since the next scheduled meeting on September 16th coincides with COVITS, it will be rescheduled and that information will be sent out at a later time.

Adjourn

Upon a motion by Mr. Kestner and duly seconded by Mr. Adkins, the Committee meeting was adjourned at 11:21am.