Report on the Virginia Information Sharing and Analysis Organization
November 2016

Introduction. This report documents the development and implementation status of the Virginia Information Sharing and Analysis Organization (VA-ISAO). In April 2015, Governor McAuliffe announced the creation of the VA-ISAO, the first public and private sector cyber sharing and analysis organization to be created by a state or commonwealth. During the FY16 legislative session, the Commonwealth of Virginia allocated $750,000 from the general fund to stand up the VA ISAO; $250,000 for FY17 and $500,000 for FY18.

Roles and Responsibilities.

The contract for the VA ISAO is being managed by the Center for Innovative Technology (CIT) – Ed Albrigo (President and CEO) and his team is supporting the effort. The Secretary of Technology for Virginia, Ms. Karen Jackson, is providing direction from the governor's office.

Existing and emerging Information Sharing and Analysis Organizations are successful if they are able to gather participation from a broad set of partners which provides important insight into threats and access to peer and near-peer organizations. The VA ISAO can gain substantial benefit from leveraging a regional resource that can draw upon participant's experiences from across the entire region bringing these benefits to the entire state of VA at a lower per participant cost. The VA ISAO will leverage the Mid-Atlantic Cyber Center (MACC) to implement and operate the VA-ISAO. Cyber adversaries (and businesses) operate across borders; and the Commonwealth's vision as a 'cyber Virginia' is reflected through this leverage opportunity.

The MACC is being stood up as a 501(c)(3) non-profit, cross-sector, Information Sharing and Analysis Organization that will facilitate information sharing and advance the cyber defenses of public and private organizations in the Commonwealth of Virginia, the State of Maryland, and Greater Washington D.C. area. The goal of the MACC is to minimize cyber-related business disruptions through the engagement of cross-sector participants on cyber threats and leading practices. This goal mirrors that of the VA ISAO and enables participants from the Commonwealth to be advantaged from the participation of a broader range of partners.

The VA ISAO and the MACC are looking to the expertise of the MITRE Corporation, co-headquartered in McLean, VA to stand up the MACC and the VA-ISAO. MITRE is a non-profit, independent 501(c)(3) that was created over fifty years ago, with a charter to serve the public interest. MITRE is a nationally recognized leader in cyber defense and has been a very active participant in a variety of cyber sharing organizations for nearly ten years. This includes forming and piloting regional threat sharing environments such as the Advanced Cyber Security Center (ACSC) in New England, and the Northeast Ohio Cyber Center (NEOCC). MITRE has been contracted with CIT to transfer its expertise in creating information and analysis sharing organizations to the MACC – and the VA ISAO.

The following activities are vital for the establishment of the VA ISAO:

Creating and Growing the VA ISAO Membership. Efforts are underway to identify eight to twelve public and private sector organizations to be prospective founding members. These organizations will span different industry sectors, and are recognized leaders with mature cyber programs. These organizations will serve as Founders and, as such, each Founder will contribute $50,000 and provide cyber security leadership by having an executive security resource serve on the Board of Directors. The Founders will also be Partners and will participate in the Information Sharing and Cyber Collaboration activities. At least two of these Founders will host meetings pro bono.

While soliciting Founders, MITRE will also be looking for non-founding Partners to participate in the VA ISAO. For the first year, MITRE is seeking ten to fourteen Partners across industry sectors and a broad array of cyber capabilities to participate in the VA ISAO at an annual cost of $25,000 each.

These entities and alliances with other business associations will catalyze the development of the first VA ISAO Model Cyber Collaboration Center (CCC) in the Northern Virginia area. The Virginia ISAO will be comprised of multiple geographically distributed centers with Richmond as the second location.

Information Sharing Mission. The Model CCC will begin operations in the first year. The VA ISAO's goal is to support each Partner's and the region's business operations by minimizing cyber disruptions and the impact of adversarial cyber attacks. The VA ISAO will move beyond information sharing to achieve broader cyber collaboration with the ultimate goal of supporting more effective cyber defenses for both individual Partners and the Commonwealth as a whole. Threat intelligence and other cyber information sharing will occur manually during face-to-face meetings, and automatically via a MACC-supported technology platform. In addition, the Model CCC will include Cyber Analyst support to increase the sharing value proposition for Partners, and to identify important threat trends early so as to inform the broader community, enabling them to set up the appropriate defenses before being attacked.

Three categories of services are envisioned within the VA ISAO. **Threat landscaping services** will be used to on-board prospective Founders and Partners to ensure each Partner has a timely, relevant threat picture that is informed by an independent cyber expert. The on-boarding process will also be used to form collaboration groups of organizations with similar cyber goals and cyber sharing abilities. The next category of services, **peer-to-peer sharing services** are built around manual and automated peer-to-peer cyber sharing and collaboration. This includes manual, face-to-face meetings to build trust among the region's cyber professionals at different levels in the Partner Organizations (e.g., cyber-threat analyst, CISO). It also includes automated sharing built around open standards for encapsulating and exchanging threat data. The **cyber technology services** enable Partners to access the latest advances in cyber technology. Efficient cyber defenses require automated tools to assist with a wide array of requirements from collating and filtering large amounts of data to being able to synthesize advanced cyber campaigns from disparate data and information. The cyber technology services will also help inform Partner investment decisions.

Financial Sustainability

The Business Plan is focused on the main mission of elevating the Partners and the region's overall cyber defenses. This effort will also support two other key regional cyber initiatives: Workforce Development and Cyber Innovation. These have been identified as critical cyber goals by Governor MacAuliffe and last year's report from the Virginia Cyber Security Commission.[1]

Standing up the VA ISAO requires an initial investment in order to build the membership, stand up pilot cyber services, validate the value proposition that is being offered by the services, and ultimately ensure a smooth transition from pilot to fully operational mode. The needed initial investment is being sought from both public and private sector organizations (i.e., the Founders). As the VA ISAO transitions from the pilot phase to the operational phase, the funding will transition to be entirely self-sufficient through the annual Partner fees.

[1] Commonwealth of Virginia Cyber Security Commission, *Threats and Opportunities,* First Report, August 2015