Commonwealth Joint Cyber Security Operations Center

This Joint Cyber Security Operations Center (CSOC) concept is based on the "Organizational Concept to Generate Maximum Effectiveness and Efficiency" proposal created by Rear Admiral Bob Day. The notion of 'stovepipes' of information is one which must be taken seriously by the Commonwealth especially in the area of cybersecurity. Since September 11, 2001, the Commonwealth has worked towards strengthening partnerships and collaboration between state agencies, Federal agencies, and private sector owners and operators of critical infrastructure (CI). The Virginia Fusion Center (VFC) is one such institution which was established to "share resources, expertise, and/or information to better identify, detect, prevent, and respond to terrorist and criminal activity". While the VFC focuses on physical threats, they have since established a cyber element capable of sharing raw information with federal, state, local, and private sector partners. The Virginia Department of Emergency Management (VDEM) is another state agency which facilitates the Virginia Emergency Operations Center (VEOC); an institution which is utilized during times of emergency to coordinate operational efforts before, during, and after an emergency. The VEOC is comprised of seventeen (17) Emergency Support Functions (ESFs) which are comprised of state, Federal, and private industry partners who support the management of operations throughout an event.

Though each of these institutions takes an all-hazards approach to their respective missions, they have traditionally not been oriented to deal with the growing cyber threat. The Joint CSOC concept would bring together partners from the public and private sectors to facilitate the sharing of threat and vulnerability information and the coordination of response to cyber events which impact both public and private infrastructures. In establishing this concept, it will be essential to identify key partners both within the public sector Federal, state, and local agencies as well as private sector owners and operators in Virginia. It will be equally important to define the roles and responsibilities of each participating entity, as many are yet to define their role in cyber security. The Joint CSOC should exist physically to assemble partners for enhance collaboration and information sharing, as well as a virtual environment to extend the mission to partners who might not have the capacity or geographic location to have physical representation.

Mission

To provide public and private sector participants with a common operating picture by administering a collaborative environment in which participating organizations can better coordinate and share information and resources.

Scope

The Joint CSOC would be made available to Federal, state, local, and private sector critical infrastructure partners who would be connected either physically for a period of no more than six (6) month rotations, or virtually in an effort to create and cultivate collaboration and coordination. Common operating picture should be defined as the sharing of detailed organizational threat information between participant organizations in a centralized and/or virtually connected environment for the purposes of situational awareness, investigations, resource requests and allocations, and incident response and recovery.

Objectives/Capabilities

- Share vulnerability and threat information in near real time
- Evaluate and disseminate trends and patterns in attack methodologies and techniques
- Make resource requests directly between partners
- Facilitate coordination between partners during a cyber event
- Support state and Federal investigations into cyber attacks and crimes against infrastructure and citizens
- Strengthen partnership between public sector governments and between the public and private sectors

Representatives

Entities represented in the Joint CSOC, whether physically or virtually, should include Federal, state, local, and private sector partners.

State

The core representation of state agencies in the Joint CSOC is overseen by the Secretaries of Technology and Public Safety and Homeland Security. The Center should have representation from each secretariat as well as their respective agencies.

- Office of the Secretary of Technology
    - Virginia Information Technology Agency (VITA)
        - VITA's Commonwealth Security and Risk Management Directorate (CSRM) is charged with the protection of the information systems utilized by all executive branch agencies
- Office of the Secretary of Public Safety and Homeland Security
    - Virginia State Police (VSP) – Virginia Fusion Center Cyber Security Unit and High Tech Crimes
    - Virginia National Guard (VANG)
        - Has a number of defensive and response capabilities which they are able to provide to the state; however, their role must be clearly defined in this respect
    - Virginia Department of Emergency Management (VDEM)
        - Coordinates response activities to disasters
        - Used as a conduit to activate the National Guard

Federal

- Federal Bureau of Investigation (FBI)
    - Each FBI field office has a Cyber Task Force (CTF) whose mission is "to counter threats, …synchronize domestic cyber threat investigations in the local community through information sharing, incident response and joint enforcement and intelligence actions." While the intention of the CTF is to include state and local participation, this capability is yet to be realized in Virginia

- Department of Homeland Security (DHS)
    - DHS has a number of collaboration/information sharing entities such as the National Cybersecurity and Communications Integration Center (NCCIC) who could be used as a model and a means of partnership for Federal participation
    - The expanding Cyber Security Advisor (CSA) Program

- Department of Defense (DOD)
    - Virginia is unique in the number of critical DOD assets located in the state
    - DOD has a vested interest in working with partners within the Commonwealth to ensure the security of their IT infrastructure

Locals

- A representation of localities should be present, at least virtually, to ensure that they receive up to date threat information which could potentially impact their systems
- Participation with state and Federal representatives will also strengthen relationships

Private Sector

- A representation of critical infrastructure sectors present in Virginia should have presence whether physically or virtually
    - Power Companies – e.g. Dominion Virginia Power
    - Telecommunications – e.g. Verizon
    - Datacenters – e.g. Raging Wire
- Can provide in-kind subject matter expertise
- Means of promoting private sector engagement in the Joint CSOC concept should be identified in order to garner broader participation across sectors
    - Incentivize participants
        - Tax breaks
        - Access to threat data
        - Vulnerability assessments

Colleges and Universities

- Can provide a number of resources to include research and modeling and simulation
- Has a vested interest in maintaining stability of their networks and

<u>Virtual Joint CSOC</u>

Participation should come from a wide variety of public and private sector organizations. Having a virtual platform from which the Joint CSOC may provide information on threats and vulnerabilities would benefit those entities that are not represented physically in the Center. Platforms to provide this virtual service should be researched to identify whether any exist currently or if such a platform must be developed specifically for this reason. While such a platform might not be in use for this particular purpose, there could be such a platform which might be easily tailored to fit the needs of the CSOC. Securing access to such an environment will also be necessary in order to prove that participants are who they say they are. Existing forms of two to three factor authentication should be leveraged (e.g. smart card or Key Fob) to increase the level of assurance to users who are granted access to such a

system. For more details on the Virtual Joint CSOC concept, please see the proposal titled "Initial Concept for Commonwealth of Virginia Cyber Information Exchange and Reporting Portal".

Physical Joint CSOC

A physical center should be established to facilitate participation from key parties from the state government as well as Federal and private sector organizations. A delegation from VITA, VSP, and VANG should be present in the CSOC at all times and should facilitate its operations on a day to day basis. Representatives from other agencies within the Federal, state, or local governments may be present as well as delegations from private lifeline sector entities. An ideal location for the Joint CSOC must be identified which provides convenience, security, and fosters broad participation of all partners.

In order to establish the Joint CSOC, a core group of state agencies (i.e. Governor's Office, VITA, VSP, and VANG) should form the initial representation in the Center. As the Joint CSOC develops, additional representatives from the Federal government, local governments, and private sector may be included to strengthen the level of information being shared. To alleviate any hindrances caused by the sensitivity of the information being shared, any information which is disseminated in the Joint CSOC should be kept at the *For Official Use Only* (FOUO) classification and shall not exceed the *Law Enforcement Sensitive* (LES) marking. All participating organizational representatives must also complete and pass a Virginia State Police (VSP) back ground investigation in order to be seated physically in the Joint CSOC.

The concept includes organizational representatives monitoring their threat information remotely from a centralized location and having the ability to provide details regarding threats facing their respective organization. The threat information will be shared; however, the data will remain in the possession of the organization and will not be centrally collected. All information can be shared using a common viewable area. In order to establish such an environment, there are general resources and infrastructure with associated costs which must be identified in acquired.

As stated, the Joint CSOC will be established using a phased approach with a core set of state agency representatives participating initially, expanding later to engage private sector owners and operators and potentially other entities such as localities. It is estimated that the initial cost for the CSOC will be $107,700.35 to establish the infrastructure required for the Center's physical environment. This estimate was determined through a number of factors to include personnel, equipment, and facility space.

Total cost to establish the Joint CSOC: $544,700.35 with an operational cost of $467,790.00 annually.

- Personnel *

Personnel	Cost
CSOC Manager	$100,000
CSOC Assistant Manager	$80,000
VITA Participant	$117,000
VANG Participant (w/o fringe)	$70,000
VSP Participant (w/o fringe)	$70,000
Total	**$437,000**

- Equipment

Equipment	Quantity	Cost
CSOC Infrastructure	1	$35,000.00
Server & storage *	1	$20,000.00
Work Stations **	5	$8,285.35
Email (Secure) *	5	$165.00
Total		**$63,450.35**

- Facility

Facility Space	Cost
Secured Work Space Upgrade	$40,000.00
Work Space Rent	$4,250.00
Total	**$44,250.00**

* Costs are annual in order to conduct operations of the Join CSOC

** Cost of the annual workstation of $1,275 per year plus a $382.07 fee per every four years per workstation

Assumptions

The costs calculated for the establishment and operations of the Joint CSOC were made based upon several assumptions. In order to calculate a rough estimate of the cost of facility space and facility upgrades, it was assumed that the Center would be established in the Public Safety and Homeland Security section of the Patrick Henry Building. While there were several viable alternatives to this facility, the space in the Patrick Henry Building has:

1. Secure space which is relatively unused and can be leveraged for the purposes of the Joint CSOC
2. Having the Center physically located with the Technology and Homeland Security and Public Safety Secretariats, heightens its visibility and provides for greater access of information to decision makers as well as enhanced collaboration among participating agencies.
3. The Patrick Henry Building is located centrally in Downtown Richmond and can be easily accessed by participants from both the public and private sector while remaining secure from unauthorized individuals
4. The Center would coincide with the proposed Homeland Security Joint Staff which will be housed in the same location, allowing for further collaboration with entities serving a homeland security mission

The cost of equipment and infrastructure was calculated by partners from VITA who have extensive experience in establishing Security Operation Center (SOC) environments. Costs for equipment are a combination of one time purchases of infrastructure to facilitate monitoring and communication as well as standard costs for the utilization of equipment from the VITA/Northrop Grumman partnership (e.g. laptops).

Rough estimates for the budgeting of personnel were calculated on an individual agency basis. Each agency estimated the cost of providing the support of one qualified employee for a six month rotation. Although the goal is to garner voluntary participation from partners, agencies such as VITA and VSP do not currently have adequate staff to supply for a six month rotation and would require the hiring of an additional employee to facilitate this staffing. For VANG to staff the Center they will require the service member to be under state active duty status and thus the Commonwealth will have to pay for the cost of that qualified person to participate. It is also assumed that the Center will operate during normal business hours with the understanding that in the event of an emergency, staff will be made available.